OVERCOMING INFORMATION OPERATIONS LEGAL LIMITATIONS IN SUPPORT OF DOMESTIC OPERATIONS

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
Homeland Security Studies

by

PETER L. ELSTAD, MAJ, USA
B.A., Winona State University, Winona, Minnesota, 1988

Fort Leavenworth, Kansas
2008

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-12-2008	Master's Thesis	FEB 2008 – DEC 2008

4. TITLE AND SUBTITLE
Overcoming Information Operations Legal Limitations in Support of Domestic Operations

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Peter L. Elstad

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Overcoming information operations legal limitations in support of domestic operations is a stumbling block to applying information effectively in this environment. Current US Title 10 restrictions limit the use of certain assets (e.g. Psychological Operations PSYOP assets) against the US domestic population during times of crisis. The new FM 3-0, Operations, states that information is an element of combat power and this construct in theory allows all Army information tasks to be legally and equally applied in domestic operations. This thesis attempts to answer the question, "can Army information tasks be legally and doctrinally applied in domestic operations?" The Smith – Mundt Act of 1948, Posse Comitatus Act, Insurrection Act of 1807, Stafford Act, Title 10 of the Federal Code, and Title 32 of the Federal Code all impose legal limitations on the use of military forces in domestic operations. Army information tasks appear to fall in a gray area which requires interpretation as whether or not they can be used in domestic operations. By using content analysis, this thesis attempted to examine a broad spectrum of written opinion from various perspectives (legislative, executive branch, Department of Defense, Department of the Army, and academic / civilian). This was an attempt to get an understanding of what the overall collective opinions were regarding IO support in domestic operations. The findings indicate the collective thought (or opinion) of the 'Information Community' that it may be possible to apply Army information tasks legally in domestic operations.

15. SUBJECT TERMS
Information Operations, Domestic Operations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	75	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE
THESIS APPROVAL PAGE

Name of Candidate: MAJ Peter L. Elstad

Thesis Title: Overcoming Information Operations Legal Limitations in Support of Domestic Operations

Approved by:

_____, Thesis Committee Chair
Mr. O. Shawn Cupp, MS

_____, Member
LTC Prisco R. Hernandez, Ph.D.

_____, Member
LTC Robert F. Foley, MA

Accepted this12th day of December 2008 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

OVERCOMING INFORMATION OPERATIONS LEGAL LIMITATIONS IN SUPPORT OF DOMESTIC OPERATIONS, by MAJ Peter L. Elstad, 75 pages.

Overcoming information operations legal limitations in support of domestic operations is a stumbling block to applying information effectively in this environment. Current US Title 10 restrictions limit the use of certain assets (e.g. Psychological Operations PSYOP assets) against the US domestic population during times of crisis. The new FM 3-0, Operations, states that information is an element of combat power and this construct in theory allows all Army information tasks to be legally and equally applied in domestic operations. This thesis attempts to answer the question, "can Army information tasks be legally and doctrinally applied in domestic operations?" The Smith – Mundt Act of 1948, Posse Comitatus Act, Insurrection Act of 1807, Stafford Act, Title 10 of the Federal Code, and Title 32 of the Federal Code all impose legal limitations on the use of military forces in domestic operations. Army information tasks appear to fall in a gray area which requires interpretation as whether or not they can be used in domestic operations. By using content analysis, this thesis attempted to examine a broad spectrum of written opinion from various perspectives (legislative, executive branch, Department of Defense, Department of the Army, and academic / civilian). This was an attempt to get an understanding of what the overall collective opinions were regarding IO support in domestic operations. The findings indicate the collective thought (or opinion) of the 'Information Community' that it may be possible to apply Army information tasks legally in domestic operations.

ACKNOWLEDGMENTS

This thesis could not have been executed, let alone conceived if it were not for the assistance of two organizations: National Guard Bureau's Army Operations Division, Information Operations Branch (NGB-ARO-IO) and the United States Army Information Operations Proponent (USAIOP). Special thanks to the NGB-ARO-IO Branch Chief, LTC Larry Juhl, who originally noted there was a lack of consensus and guidance in utilizing Army information tasks in support of domestic operations. Special thanks must also go to the USAIOP Leader Development, Education, and Training Division for providing input and assistance regarding sources and developing Army information doctrinal concepts.

TABLE OF CONTENTS

Page

ACRONYMS

ARNG	Army National Guard
ARNORTH	US Army Northern Command
CINC	Commander-in-Chief
FORSCOM	US Forces Command
HQDA	US Department of the Army
IO	Information Operations
NGB	National Guard Bureau
NGB-ARO-IO	National Guard Bureau, Operations Division, Information Operations Branch
NORTHCOM	US Northern Command
OIF	Operation Iraqi Freedom
OEF	Operation Enduring Freedom
POTUS	The President of the United States
USAIOP	US Army Information Operations Proponent
USARC	US Army Reserve Command
USJFCOM	US Joint Forces Command US Forces Command
USSTRATCOM	US Strategic Command

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER ONE

INTRODUCTION

Background

According to FM 3-0, Operations, information is now an element of combat power that must be integrated into the concept of operations through the operations process. The term 'Information Operations' (or IO) is relatively new to the lexicon of the US military. Nevertheless, the US Army has a long-standing history of using the concept of information as a weapon in order to influence the outcome of campaigns and battles (Wright and Reese, 2008, p. 274).

In the 1990's, IO consisted of the integrated activities of psychological operations, operations security, public affairs, electronic warfare, military deception, and others. They were considered a means of attacking an enemy's command, control, and communications systems through these disparate activities. In 2008, this has matured to the current concept of integrated tools or processes a commander may employ to address not only enemy combatant forces, but more importantly, those entities who may provide support, sanctuary, or at a minimum, implied support by remaining neutral (Wright and Reese, 2008, p. 275).

This has been applied in past overseas deployments such as Operation IRAQI FREEDOM – OIF (Iraq), Operation ENDURING FREEDOM – OEF (Afghanistan), and in the Balkans (IFOR, SFOR, KFOR). For example, in Bosnia (as well as Afghanistan and Iraq - 'Post major combat operations'), IO had two purposes: establish credibility and legitimacy in the international community for current and planned military operations;

informing or influencing local and regional friendly, neutral favor of coalition military and interagency activities (Wright and Reese, 2008, p. 277).

Despite extensive experience with overseas stability operations, foreign military training missions, and other theater security cooperation activities, no serious thought has been given on how to leverage information in domestic operations, such as in the relief efforts for Hurricane Katrina in 2005. The Army National Guard (ARNG) has traditionally performed the homeland security/homeland defense mission and is the state governors' force for domestic operations. The ARNG, in addition to providing forces for overseas deployments (as an operational reserve), is also being called upon to support non-traditional missions, including but not limited to providing security for major events (e.g. Bird Flu Pandemic). Over 50% of the Army's force structure is located in the ARNG. Considerations for applying information in this environment have been an oversight in the past.

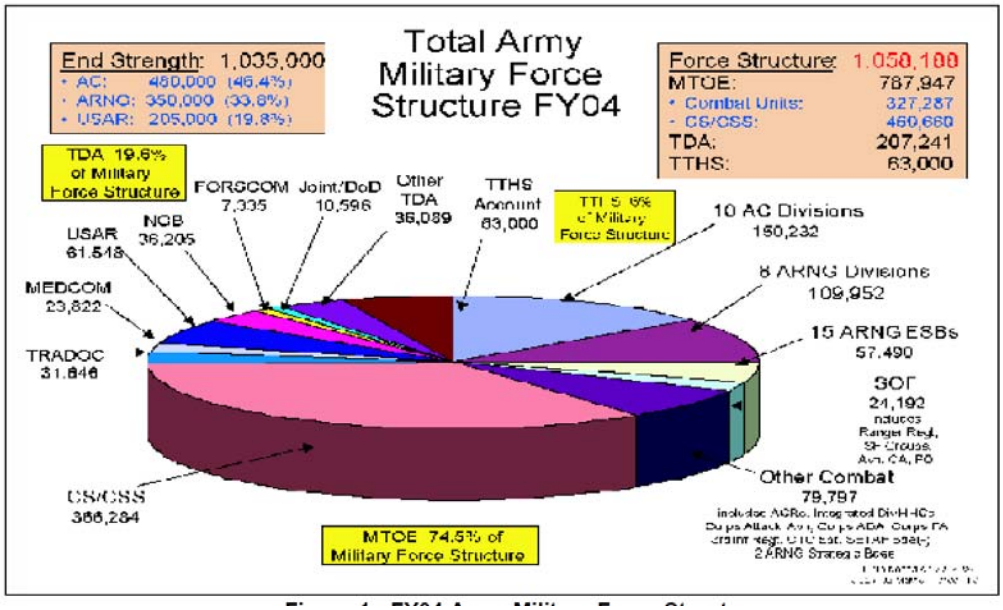

Figure 1. Total Army Military Force Structure FYO4
Source: 2003 Army Modernization Plan 2003 (Figure 1, Appendix B, Washington, DC: Government Printing Office, February 2003), p. B-1.

The primary question that must be addressed is: Can information tasks be legally and doctrinally applied in domestic operations? In order to answer this question, related aspects pertaining to this question must be addressed. First, what historical examples from the recent past (1999 to the present) yield common insights that could be applied to future domestic operations? Second, given common threads between historical operational examples, what was the relative effectiveness in employment of information in these situations based on common measures of success? Third, what are the current legal restrictions for performing Army information tasks: e.g. Information Engagement, Command and Control Warfare, Information Protection, Operations Security, and Military Deception in domestic operations? Finally, there must be an examination of what common threads exist between operational historical examples in the application of information operations concepts to domestic operations.

Significance

This thesis focuses on understanding how information as an element of combat power in domestic operations is critical to mission success. By and large, domestic operations will consist of non-lethal options and activities. Mission commanders and military planners must seek to create asymmetrical advantages in order to offset the inability to use lethal force. In domestic operations, lethal force must be a last resort reserved only when necessary to preserve life, limb, and critical infrastructure. Properly employed, information (as an element of combat power) provides a significant multiplier that can help the commander and his staff shape and impose his will on the Domestic Support Operational Environment.

Assumptions

Domestic support operations since 1999 have consisted of actions and activities that resemble similar operations that the United States (unilaterally, or as part of a coalition) has conducted under the name of stability operations. The likelihood of the United States having to fight a conventional 'force on force' operation with a 'like' partner on US soil is very slim. Current conventional wisdom speculates that operations on domestic soil will consist of military support to civil authorities, humanitarian assistance, maintenance of civil order, and protecting critical infrastructure.

Definitions

Definitions of major terms are listed in this chapter; additional terms can be found in the glossary (p. 76)

Civil Support**:** Support to U.S. civil authorities for domestic emergencies, and for designated law enforcement agencies and other activities (JP 1-02). Civil support includes operations that address the consequences of natural or man-made disasters, accidents, terrorist attacks, and incidents in the United States and its territories. Army forces conduct civil support operations when the size and scope of events exceed the capabilities of domestic civilian agencies.

Table 1. Civil Support Operations	
Primary Tasks	**Purposes**
• Provide support in response to disaster or terrorist attack	• Save lives
	• Restore essential services
• Support civil law enforcement	• Maintain or restore law & order
	• Protect infrastructure & property
• Provide other support as required	• Maintain or restore local government
	• Shape the environment for interagency success

Table 1. Army Civil Support Operations Tasks and Purposes

Source: FM 3-0, Operations (Figure 3-2, the Elements of Full Spectrum Operations, Washington, DC: Government Printing Office, February 2003), p. 3-7.

Army forces conduct civil support operations domestically and stability operations overseas, even though stability and civil support operations have many similarities (FM 3-0, 2008, p. 3-7, pp. 3-17 to 3-19).

Combat Camera: The acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services (FM 3-0, 2008, p. Glossary-3).

Command and Control Warfare (C2W): The integrated use of physical attack, electronic warfare, and computer network operations, supported by intelligence, to degrade, destroy, and exploit an enemy's or adversary's command and control system or to deny information to it (FM 3-0, 2008, p. Glossary-4).

Domestic Support Operations: Those activities and measures taken by the Department of Defense to foster mutual assistance and support between the Department of Defense and any civil government agency in planning or preparedness for, or in the application of resources for response to, the consequences of civil emergencies or attacks, including national security emergencies (FM 1-02, 2004, p. 1-66).

Electronic Warfare (EW): Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).

a. Electronic attack—That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams), or antiradiation weapons.

b. Electronic protection—That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of

friendly or enemy employment of electronic warfare that degrade, neutralize or destroy friendly combat capability.

c. Electronic warfare support—That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence (FM 1-02, 2004, p. 1-69).

Full Spectrum Operations: (The Army's Operational Concept) Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and informed by a thorough understanding of all variables of the operational environment. Mission command that conveys intent and an appreciation of all aspects of the situation guides the adaptive use of Army forces (FM 3-0, 2008, p. 3-1).

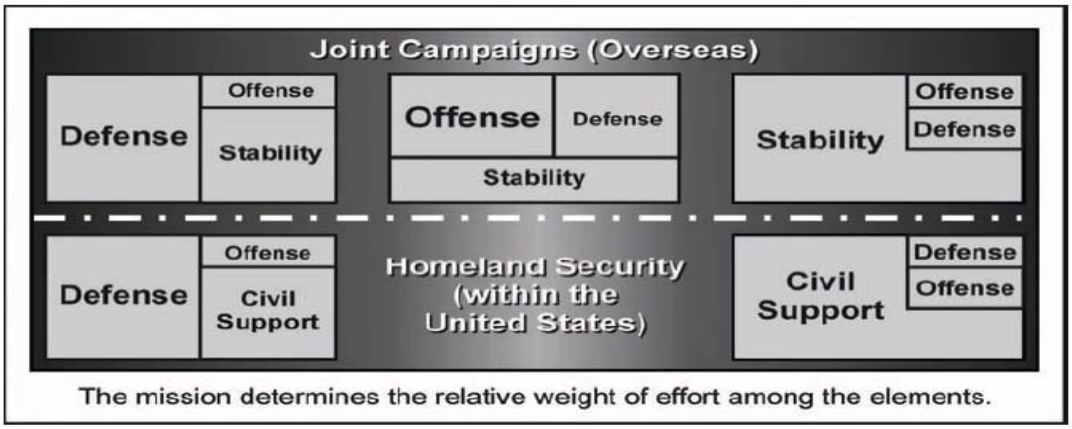

Figure 2. Full Spectrum Operations
Source: FM 3-0, Operations (Figure 3-1,Full Spectrum Operations – the Army's operational concept, Washington, DC: Government Printing Office, February 2003), p. 3-1.

Information: In the general sense, the meaning humans assign to data. In the context of the cognitive hierarchy, data that has been processed to provide further meaning (FM 1-02, 2004, pp. 1-98 to 1-99)

Information Engagement (IE): The integrated employment of public affairs to inform U.S. and friendly audiences; psychological operations, combat camera, U.S. Government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign audiences; and, leader and Soldier engagements to support both efforts (FM 3-0, 2008, p. glossary-7).

Information Operations: The employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect and defend information and information systems and to influence decision making (FM 1-02, 2004, p. 1-99).

Information Protection: Active or passive measures that protect and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information. It denies enemies, adversaries, and others the opportunity to exploit friendly information and information systems for their own purposes (FM 3-0, 2008, p. glossary-7).

Military Deception (MILDEC): Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or refraining from taking actions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are as follows:

a. Strategic Military Deception—Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations.

b. Operational Military Deception—Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater to support campaigns and major operations.

c. Tactical Military Deception—Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements.

d. Service Military Deception—Military deception planned and executed by the Services that applies to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems.

e. Military Deception in Support of Operations Security (OPSEC)—Military deception planned and executed by and in support of all levels of command to support the prevention and inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or to provide cover for, military operations and activities (FM 1-02, 2004, p. 1-123).

Operations Security (OPSEC): A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Note: the Army replaces "critical information" with "essential elements of friendly information." (FM 1-02, 2004 pp. 1-140 to 1-141).

Psychological Operations (PSYOP): Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups,

and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives (FM 1-02, 2004, pp. 1-152 to 1-153).

Stability Operations: Operations that promote and protect US national interests by influencing the threat, political, and information dimensions of the operational environment through a combination of peacetime developmental, cooperative activities and coercive actions in response to crisis (FM 1-02, 2004, p. 1-175, FM 3-0, p. 3-7).

Table 2. Stability Operations	
Primary Tasks	**Purposes**
• Civil security	• Provide for a secure environment
• Civil control	• Secure land areas
• Restore essential services	• Meet the critical needs of the populace
• Support to governance	• Gain support for host-nation government
• Support to economic and infrastructure development	• Shape the environment for interagency and host-nation success

Table 2. Stability Operations Tasks and Purposes.

Source: FM 3-0, Operations (Figure 3-2,the elements of full spectrum operations, Washington, DC: Government Printing Office, February 2003), p. 3-7.

Strategic Communication: Focused United States Government (USG) efforts to understand and engage key audiences in order to create, strengthen or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power (JP 3-13, 2006, p. GL-12).

Limitations

This thesis will limit itself to examining historical case studies from 1999 to 2007. The year 1999 is significant because that year coincides with publication of the Army's first Information Operations Doctrine, FM 100-6 (Information Operations). FM 100-6 represented the Army's first attempt to codify and nest information related disciplines such as PSYOP, Public Affairs, Electronic Warfare, Military Deception, Operations Security, and Computer Network Operations with operational maneuver forces' actions (referred to as 'physical destruction'). It is difficult to examine case studies prior to 1999 since the Army did not have a coherent doctrine prior to this date that could be used to frame the discussion.

Delimitations

This thesis will not discuss information operations from a joint or other service perspective and instead will focus on the Army's viewpoint as the land component. The Army's perspective is unique because unlike the other services (Air Force, Navy), the Army 'lives with its target audiences' before, during, and after operations. FM 3-0, Chapter 7 recognizes this by stating, "…Army forces contend constantly with the attitudes and perceptions of populations within and beyond their area of operations. Commanders use information engagement in their areas of operation to communicate information, build trust and confidence, and promote support for Army operations, and influence perceptions and behavior." (FM 3-0, 2008, Chapter 7, p. 7-3).

This thesis will not address Army operations conducted outside Title 10 and Title 32 authority, as in the case of National Guard forces operating in 'state active duty' under authority of their respective governors. Such examination is best left to another study

due to the complexity presented by the 54 different codes of military conduct of each US state and territory. This thesis will not review or consider information operations sources that are classified or considered 'FOR OFFICIAL USE ONLY'. This is to ensure the widest dissemination of this thesis in order to foster future discussions and dialogue with the intent of further influencing future Army doctrine.

In chapter four, this thesis will address understanding how the Army could conceivably employ information as an element of combat power in domestic operations. Chapter two examines current literature on information operations. The first step will be to examine what is the current, accepted 'institutional' definition, or rather interpretation, for information operations (how does the Army apply IO), versus any emerging doctrinal definition.

CHAPTER 2

LITERATURE REVIEW

Chapter one postulated that information is now an element of combat power that must be integrated into the concept of operations through the operations process. The US Army has previously used information to influence the outcome of military operations since the 1990's. IO has matured in the last two decades from a way of attacking an enemy's command, control, and communications systems to the current concept of integrated tools a commander may employ to inform or influence local and regional friendly, neutral and adversarial audiences in favor military operations.

In order to understand how the Army could conceivably employ information as an element of combat power in domestic operations, an examination of current literature is required. The first step is to examine what the current, accepted 'institutional' definition, or rather interpretation, for information operations (how does the Army apply IO), versus any emerging doctrinal definition. This is critical because it takes time for the Army as an institution to accept and embrace new concepts (Nagl, 2002, pp. 3-6).

In chapter one, the Army defined Information Operations as, "[The] employment of core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect and defend information and information systems and to influence decision making." (FM 1-02, 2004, p. 1-99).

Additionally, FM 3-0 states that the Army would employ information operations by way of five tasks (Information Engagement, Command and Control Warfare, Information Protection, Operations Security, and Military Deception), and provided the

following framework to explain conceptually its application. FM 3-0 could not stress more the importance of information and the importance of peoples' beliefs, perceptions, and behaviors in influencing the success or failure of Army operations:

Task	*Information Engagement*	*Command and Control Warfare*	*Information Protection*	*Operations Security*	*Military Deception*
Intended Effects	•Inform and educate internal and external publics •Influence the behavior of target audiences	•Degrade, disrupt, destroy, and exploit enemy command and control	•Protect friendly computer networks and communication means	•Deny vital intelligence on friendly forces to hostile collection	•Confuse enemy decision-makers
Capabilities	•Leader and Soldier engagement •Public affairs •Psychological operations •Combat camera •Strategic Communication and Defense Support to Public Diplomacy	•Physical attack •Electronic attack •Electronic warfare support •Computer network attack •Computer network exploitation	•Information assurance •Computer network defense •Electronic protection	•Operations security •Physical security •Counterintel-ligence	•Military deception

Figure 3. Army Information Tasks
Source: FM 3-0, Operations (Washington, DC: Government Printing Office, February 2008), p. 123.

Second, an examination of the definition of domestic operations is also required. The Army defines domestic operations as, "…activities and measures taken…to foster mutual assistance and support…in planning or preparedness for, or in the application of resources for response to, the consequences of civil emergencies or attacks, including national security emergencies." (FM 1-02, 2004, p. 1-66). FM 100-19, Domestic Support Operations (currently under revision as FM 3-28, Civil Support Operations) simplified this definition further as, "…the authorized use of Army physical and human resources to support domestic requirements." (Federation of American Scientists, 1993).

Having firmly established what the accepted institutional definitions are for both 'information operations' and 'domestic support operations', it is then necessary to conduct a review or examination of what the existing literature out in the field says about legal restrictions and opinions as they apply to IO. The review or examination of the information sources has a cut-off date of February 2008, as that was the date when the Army's new concept for information was published in FM 3-0, Chapter 7.

The examination began by looking at what are the perspectives of academic and civil authorities regarding the definitions of the terms of reference outlined in Chapter 1 of this thesis. The controversies regarding the use of psychological operations, military deception, and electronic warfare against the US public were also examined.

In reviewing academic and civil authority perspectives, it was worth noting the importance of legislation as possibly providing limitations to the use of information and performance of information tasks (psychological operations, military deception, and electronic warfare in particular) in domestic support operations. Federal statutes imposing such limitations include the 'Posse Commitatus Act', the 'Insurrection Act', the 'Stafford Act', and the 'Smith - Mundt Act'. Also examined were what the Army refers to as 'Title 10' and 'Title 32' authority to see if there were any additional applicable limiting legislation.

The President of the United States (POTUS) as Commander-in-Chief (CINC) of US Armed Forces has responsibility through the Executive Branch of government to provide guidance and direction for the application and use of military forces. This also includes domestic support operations. This required examination of applicable Executive Branch guidance and policies including Homeland Security Presidential Directives

(HSPDs); Department of Homeland Security (DHS) guidance and policies; and Federal Emergency Management Agency (FEMA) policies.

Executive Branch policy and guidance review must also include examining Department of Defense (DOD) guidance, policy, and directives. The expectation was that this review would not yield limiting factors (as in legislative review), but rather provide guidance to determine under what circumstances and how information tasks could be performed. The last Quadrennial Defense Review (2006) was also examined as starting point, and was followed by a review of joint doctrine. Combatant command guidance: US Joint Forces Command - USJFCOM, US Forces Command - FORSCOM, US Strategic Command - USSTRATCOM, US Northern Command - NORTHCOM, and US Army Northern Command - ARNORTH was also reviewed. The examination also reviewed US Department of the Army - HQDA, US Army Reserve Command - USARC, and National Guard Bureau - NGB guidance and policy.

The literature review appeared to have adequate depth and breadth to proceed with analysis and attempt to answer the original thesis question: Can information tasks (information engagement, command and control warfare, military deception, information protection, and operations security) be legally applied in domestic operations? The next chapter describes a research methodology that should permit exploration and analysis framed around these focus areas:

- Legal restrictions for planning, preparing, executing and assessing the effectiveness of Army information tasks (information protection, military deception, operations security, command and control warfare, and information engagement) in domestic support operations.

- Common threads (or insights) from recent history (1999 to the present) that could be applied to future domestic operations.
- Parallels between operational historical examples (domestic operations and overseas stability operations).

CHAPTER 3

RESEARCH DESIGN

This thesis declared in Chapter one that information is an element of combat power that commanders and staffs must integrate into the concept of operations through the operations process spelled out in FM 3-0, Operations. Since the 1990's, US Army has used information to influence the outcome of military operations. It has moved from a methodology of attacking an enemy's command, control, and communications systems to a concept of integrated tools a commander may employ to inform or influence local and regional audiences (friendly, neutral, and adversaries) in favor military operations.

The literature review outlined in Chapter two appeared to have adequate depth and breadth to proceed with analysis and attempt to answer the original thesis question: Can information tasks (information engagement, command and control warfare, military deception, information protection, and operations security) be legally applied in domestic operations? Chapter three describes a research methodology that should permit exploration and analysis framed around these focus areas:

- Legal restrictions for planning, preparing, executing and assessing the effectiveness of Army information tasks (information protection, military deception, operations security, command and control warfare, and information engagement) in domestic support operations.
- Common threads (or insights) from recent history (1999 to the present) that could be applied to future domestic operations.
- Parallels between operational historical examples (domestic operations and

overseas stability operations).

After consultation and reviewing various research design methods, it was determined that content analysis methodology would be the best research design to examine existing writing on this topic. According to Bruce Berg in his book Qualitative Research Methods for the Social Sciences, content analysis consists of "…careful detailed, systematic examination and interpretation of a particular body of material in an effort to identify patterns, biases, and meanings." (Berg, 2007, pp. 303 - 304).

Under the assumption that the U.S. Army, and by extension, the civil authorities it answers to (e.g. Department of Defense, Executive Branch, Legislative Branch, etc) constitute a social culture, then a social anthropological approach would be an appropriate strategy for this study. Content analysis with a social anthropological approach would be the best approach used by researchers who have spent considerable time in a given community, and have participated in various activities, either directly or indirectly, with many of the individuals within that community to be studied.

The task, according to Berg, would then be to identify and explain the ways people use or operate in a particular setting. In this case, it is the Army, applying information tasks in a domestic support operation and understanding the thought and logic in the application of these information tasks (Berg, 2007, p. 304).

The information necessary for this research did not require outside collection of external data. Content analysis offered several advantages:

1. It would be unobtrusive — by reviewing existing writing and thought within the limitations and delimitations listed in chapter one, it would be possible to examine the amount of emphasis each source placed on certain themes and concepts. Additionally, by

examining these themes and concepts, it would also be possible to gain understanding of the context of the writing by the sources' expressed opinion.

2. It would be cost effective — no additional studies or surveys would be necessary. All data sources could be found via research through the Combined Arms Library (CARL) at Fort Leavenworth, KS.

3. It would provide a means to study the evolution of collective thought by the Army during the envisioned study period (1999 to 2008) by examining the existing public record: e.g. documentation available open-source and available to the general public.

The data collection and analysis process would be conducted from an open-ended viewpoint, and used a deductive approach. This approach could make it possible to ensure impartial, untainted, and unbiased conclusions regarding the original research question: Can information tasks be legally and doctrinally applied in domestic operations?

To summarize, the first step in research was to define the range of existing writing to be examined. In order to keep this range of materials to a manageable level, the examination was limited to writings from 1999 to 2008. The year 1999 served as a useful limit, as that year marked the first time the Army conducted stability operations in the Balkans. This is where the Army began utilizing IO concepts in their present form. The year 2008 served as a good limitation, because that was when FM 3-0 was published and the Army adequately described how information as an element of combat power could support full spectrum operations.

The second step after defining the range of existing writing was do determine a series of filters or sieves that could initially determine if a data source contained content worth analyzing. These series of filters were initial screening criteria based on the six proposed perspective areas:

Table 3. Perspective Areas and Screening Criteria						
Legislative Perspective	Title 10 Authority	Title 32 Authority	Posse Comitatus	Insurrection Act	Stafford Act	Smith - Mundt Act
Executive Branch Perspective	HSPD	Other Exec Orders	DHS Guidance & Policies	FEMA Guidance & Policies	QDR	
Dept of Defense Perspective	DSCA Guidance	Joint Doctrine	Combined Doctrine	Army Doctrine		
Combatant CDR's Perspective	USJFCOM Guidance	USSTRATCOM Guidance	FORSCOM Guidance	NORTHCOM Guidance		
HQDA Perspective	HQDA Guidance	USARC Guidance	NGB Guidance			
Academic & Civilian Perspective	Terms of Reference	Propaganda Issues	Legal Issues	Homeland Security & Defense Issues		

Table 3. Perspective Areas and Screening Criteris

Source: Created by Author

If upon reviewing a data source with these screening criteria resulted in finding writing on this topic area, the data source would be set aside for a subsequent review. This subsequent review would then determine if this data source had anything to say regarding Army Information Tasks.

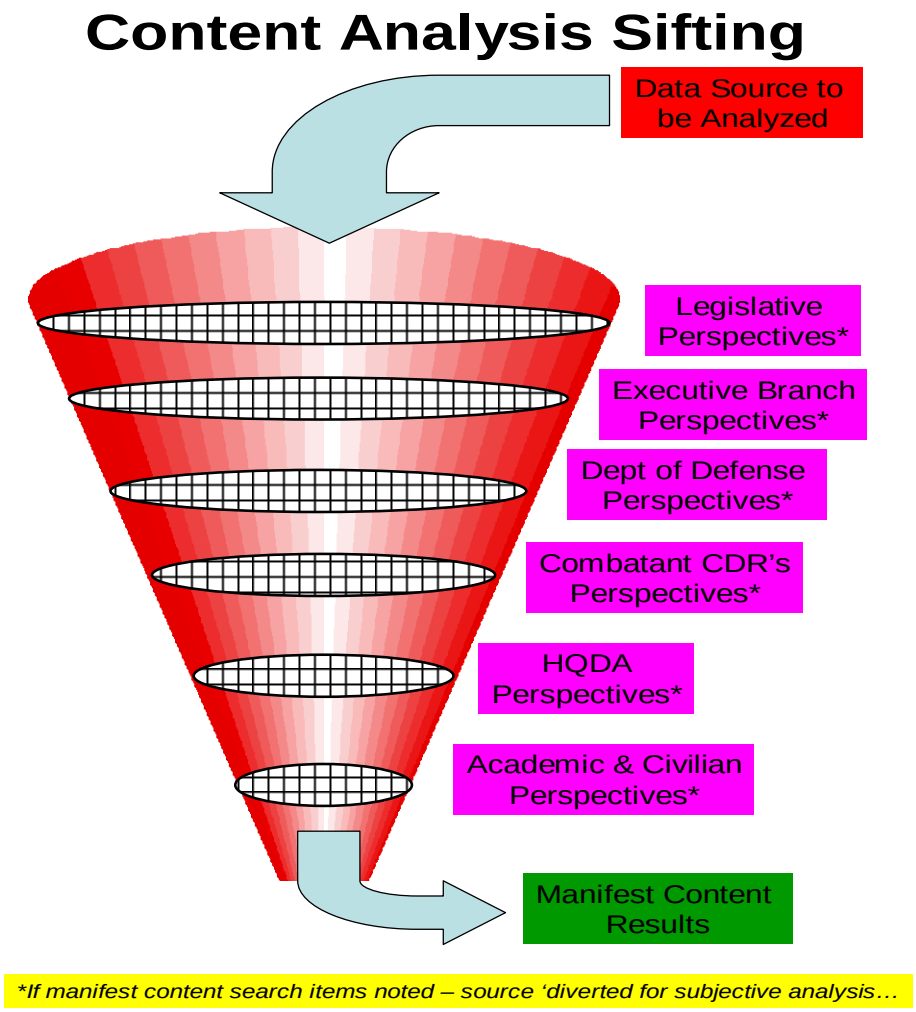

Figure 4. Content Analysis Sifting
Source: Created by Author

The second step in content analysis research design would then be to determine what to look for or count. Commonly accepted practice for content analysis methodology is also to look at '***themes***' and '***concepts***'. The American Heritage Dictionary defines themes as "…a topic of discourse or discussion." Berg defines concepts as "…words grouped together into conceptual clusters (ideas)…" (Berg, 2007, p. 313).

The ***five information operations tasks*** defined in Chapter One (Information Engagement, Command and Control Warfare, Military Deception, Information

Protection, and Operations Security) ***would serve as themes*** for this analysis. ***Army information capabilities*** that support Army information tasks (outlined in FM 3-0) would ***serve additionally as concepts*** for this analysis.

Table 4. Army Information Tasks and Capabilities					
TASK	Information Engagement	Command and Control Warfare	Information Protection	Operations Security	Military Deception
CAPABILITY	Leader & Soldier Engagement	Physical Attack	Information Assurance	Operations Security	Military Deception
	Public Affairs	Electronic Attack	Computer Network Defense	Physical Security	
	Psychological Operations	Electronic Warfare Support	Electronic Protection	Counter Intelligence	
	Combat Camera	Computer Network Exploitation			
	Strategic Communications				

Table 4. Army Information Tasks and Capabilities

Source :FM 3-0, Operations. (Washington, DC: Government Printing Office, February 2008), p. 123.

The third step was to examine the collection of raw survey data in some type of hierarchical order based on the related questions specified in chapter one. After some initial source review, it was determined that the original sequencing in addressing the related aspects of our original thesis question from chapter one was in the wrong order. The original thesis question asked: Can information tasks be legally and doctrinally applied in domestic operations? In order to answer that question, it must be determined which, if any, of the Army's information tasks and/or capabilities is prohibited by law in domestic support. Once this is completed, it is necessary to examine Executive Branch policy guidance from this same perspective to define the types of domestic operations the

Army could be expected to support unilaterally or as part of a joint and/or interagency operation. The fourth step would be to determine what potential assets the Army has to perform IO by reviewing Department of Defense and Army guidance, along with any constraints that may apply.

The final step would be to conduct a review of writing by academic and civil authorities. This would include historical examples of previous Army domestic operations that either did or did not use IO and compare similarities and differences between overseas stability operations and domestic operations conducted inside the United States. Figure 5 summarizes the process:

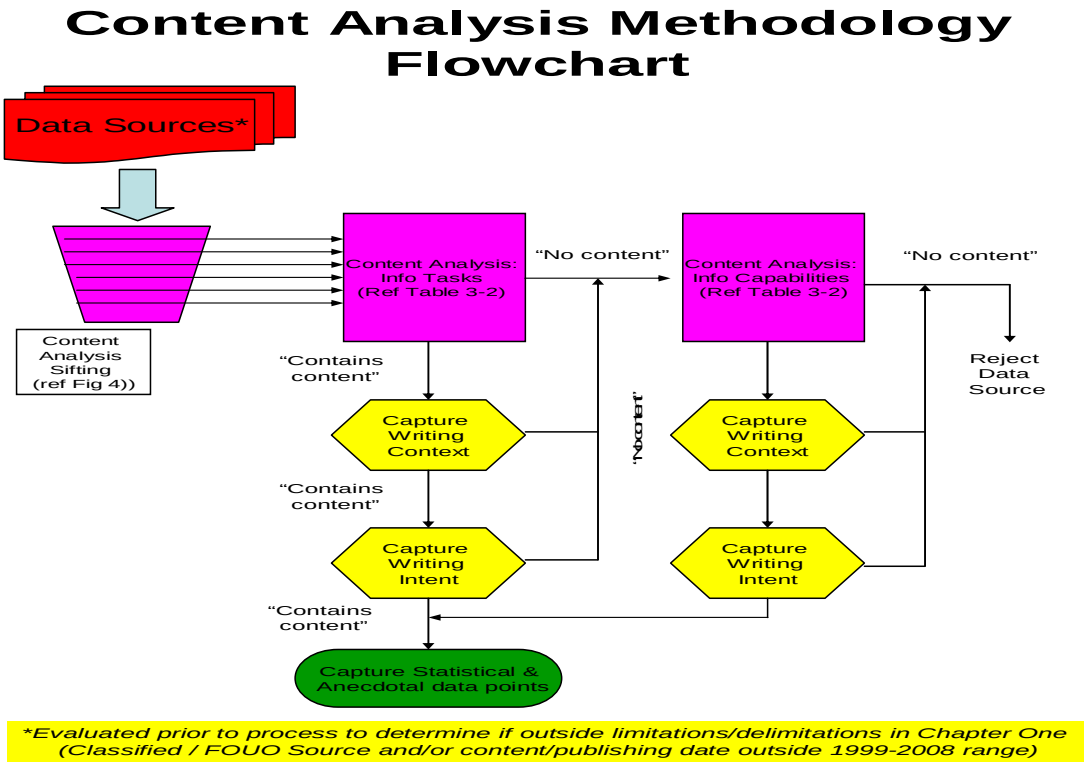

Figure 5. Content Analysis Methodology Flowchart

Source: Created by Author

Based on this analysis, there would be a good representation of the collective thought of the Army 'society' regarding the use of IO. Comparing these findings with current doctrinal practices would then allow identification of what modifications, if any would permit IO to be used in domestic operations.

Subsequent pages of this chapter describe the data coding rubrics used for conducting content analysis. Below is an example of the model that was applied to six perspective areas as rubrics: Legislative Perspectives, Executive Branch Guidance Perspectives, DOD (Joint & Army Doctrine), Combatant Command Guidance, Department (HQDA, FORSCOM, USARC & NGB) Guidance, and Academic & Civil Authorities Perspectives.

Figure 6. Rubric Perspective Example

Source: Created by Author

This rubric attempted to describe the relationship not only between absolutes, but the prevailing viewpoint on specific perceptions of the topic area; in this case, whether there is consistency between what the law absolutely describes and whether there are any areas of ambiguity which could leave the final determination open to interpretation. The analysis would also additionally include descriptions of anecdotal data observed from sources that would either illustrate consistency with the overall perception or point out inconsistencies in collective thought.

Having described the research design approach used for this study, chapter four will analyze the following six perspectives and record trends and correlations:

- Legislative Perspectives (Federal Laws and Statutes)
- Executive Branch Perspectives (Executive Orders, Presidential Directives, and Cabinet Policies)
- Department of Defense Perspectives (Review of Joint, Combined, and Army Doctrine; as well as Defense Support to Civil Authorities Guidance)
- Combatant Command Perspectives (Joint Forces Command, Strategic Command, Forces Command, Northern Command, and US Army Northern Command)
- Department Perspectives (Headquarters, Department of the Army - HQDA; US Army Reserve Command - USARC; National Guard Bureau - NGB)
- Academic & Civilian Perspectives

CHAPTER 4

ANALYSIS

Recalling Chapter one, FM 3-0, Operations, stated that information is an element of combat power that commanders and staffs must integrate into the concept of operations through the operations process. The US Army has used information to influence the outcome of military operations from the Balkans in the late 1990s, to Iraq (OIF) and Afghanistan (OEF). It has moved from a methodology of attacking an enemy's command, control, and communications systems to a concept of integrated tools a commander may employ to inform or influence local and regional audiences (friendly, neutral, and adversaries) in favor military operations. The original thesis question asked: Can information tasks (information engagement, command and control warfare, military deception, information protection, and operations security) be legally applied in domestic operations? The literature review detailed in Chapter two appeared to have adequate depth and breadth to proceed with analysis. Chapter three described the content analysis research methodology framed around three focus areas:

- Legal restrictions for planning, preparing, executing and assessing effectiveness of Army information tasks (information protection, military deception, operations security, command and control warfare, and information engagement) in domestic support operations.
- Common threads (or insights) from recent history (1999 to present) that could be applied to future domestic operations.
- Parallels between operational historical examples (domestic operations and

overseas stability operations).

Seven hundred and ninety three (793) data sources were examined, of which four hundred and forty (440) sources were rejected as not containing relevant data for content analysis. Additionally, two hundred seventy six (276) data sources were rejected because they contain material that is outside the research criteria (e.g. 'FOR OFFICIAL USE ONLY'). The remaining seventy-seven (77) data sources were analyzed, and the following sections provided summaries categorized as follows:

- Legislative (Federal Laws and Statutes)
- Executive Branch (Executive Orders, Presidential Directives, and Cabinet Policies)
- Department of Defense (Review of Joint, Combined, and Army Doctrine; as well as Defense Support to Civil Authorities Guidance)
- Combatant Command (Joint Forces Command, Strategic Command, Forces Command, Northern Command, and US Army Northern Command)
- Department (Headquarters, Department of the Army - HQDA; US Army Reserve Command - USARC; National Guard Bureau - NGB)
- Academic & Civilian

Legislative Perspectives

The first examination, legislative perspectives, consisted of coding 160 data points from eleven different sources (Figure 7).

Figure 7. Legislative Perspectives Rubric.

Source: Created by Author

The Smith - Mundt Act.

The Smith - Mundt Act is regarded as the primary legal limitation on information operations, it specifically limits psychological operations:

"The Secretary [of State] is authorized, when he finds it appropriate, to provide for the preparation, and dissemination abroad, of information about the United States, its people, and its policies, through press, publications, radio, motion pictures, and other information media, and through information centers and instructors abroad. Subject to subsection (b) of this section, ***any such information*** (other than "Problems of Communism" and the "English Teaching Forum" which may be sold by the Government Printing Office) ***shall not be disseminated within the United States, its territories, or possessions***, but, on request, shall be available in the English language at the Department of State, at all reasonable times following its release as information abroad, for examination only by representatives of United States press associations, newspapers, magazines, radio systems, and stations, and by research students and scholars, and, on request, shall be made available for examination only to Members of Congress." [Emphasis Added] (Legal Information Institute, 2007).

Title 10 and Posse Comitatus.

Title 10 Authority does not clearly state any provisions regarding limiting information operations in domestic support. However, the Posse Comitatus Act does imply potential limitations on counter-intelligence: "Questions regarding which activities violate the Posse Comitatus Act arise most often in the context of assistance to civilian police. At least in that context, the courts have held that, absent a recognized exception, the Act is violated (1) when civilian law enforcement officials make "direct active use" of

military investigators, (2) when the use of the military "pervades the activities" of the civilian officials, or (3) when the military is used so as to subject citizens to the exercise of military power that is "regulatory, prescriptive, or compulsory in nature." (Best and Elsea, 2008, p.20).

Title 32 Authority.

Title 32 authority appears to provide more 'leeway' for using information operations in domestic support. This authority permits National Guard forces, not under federal mobilization, to assume the more 'police-like functions' such as protection of private property and traffic control. In addition, they are not subject to the restrictions of the Posse Comitatus act (Bazan, 2005, p. 2, & 8).

The Stafford Act.

The Stafford Act was envisioned as a flexible way to provide supplemental federal disaster relief and emergency assistance (Department of Homeland Security, 2006, p. 144). The Homeland Security Council's *Pandemic Influenza Strategy,* went so far as to say, "[I]n disaster and emergency situations, this [Stafford] Act authorizes Federal agencies to assist in the provision of State and local public health measures, including by providing logistical or materials support to State and local law enforcement… also authorizes DHS/FEMA to "*procure by condemnation or otherwise, construct, lease, transport, store, maintain, renovate, or distribute* materials and facilities for emergency preparedness," (emphasis added). The term "materials" includes "raw materials, supplies, medicines, equipment, component parts, and technical information

and processes necessary for emergency preparedness…" (Homeland Security Council, 2006, p. 225).

The Congressional Research Service also noted the Stafford Act, "…provides statutory authority for employing the U.S. armed forces for domestic disaster relief. Permitted operations include debris removal and road clearance, search and rescue, emergency medical care and shelter, provision of food, water, and other essential needs, **dissemination of public information** and assistance regarding health and safety measures, and the provision of technical advice to state and local governments on disaster management and control." (Elsea, 2005, p. 4).

Table 5. Legislative Perspective Sources Examined
Bazan, Elizabeth. *Robert T. Stafford Disaster Relief and Emergency Assistance Act: Legal Requirements for Federal and State Roles in Declarations of an Emergency or Major Disaster*. Washington, DC: Congressional Research Service, September 16, 2005.
Best, Richard A. and Jennifer K. Elsea. "Satellite Surveillance: Domestic Issues" in *CRS Report for Congress, RL34421*. Washington, DC: Congressional Research Service, March 21, 2008.
Bowman, Steve and Scott Shepard. *Homeland Security: Establishment and Implementation of the United States Northern Command.* Washington, DC: Congressional Research Service, September 8, 2005.
--, Lawrence Kapp, and Amy Belasco. *Hurricane Katrina: DOD Disaster Response.* Washington, DC: Congressional Research Service, September 19, 2005.
--. *Hurricane Katrina: DOD Disaster Response.* Washington, DC: Congressional Research Service, Updated October 6, 2005.
Elsea, Jennifer K. *The Use of Federal Troops for Disaster Assistance: Some Legal Issues.* Washington, DC: Congressional Research Service, September 16, 2005.
Homeland Security Council. *National Strategy for Pandemic Influenza Implementation Plan.* Washington, DC: Government Printing Office, May 2006.
Legal Information Institute. "TITLE 22 > CHAPTER 18 > SUBCHAPTER V > § 1461." In *U.S. Code Collection.* Cornell University Law School, January 3, 2007. http://www.law.cornell.edu/uscode/22/usc_sec_22_00001461----000-.html (Accessed May 8, 2008).
Moore, Linda K. *Public Safety Communications: Policy, Proposals, Legislation and Progress.* Washington, DC: Congressional Research Service, August 31, 2005.
US Department of Homeland Security, Office of the Inspector General. *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina.* Washington, DC: Government Printing Office, March 2006.

Table 5. Legislative Perspective Sources Examined

Source: Created by Author

Federal Government Executive Branch Perspectives

The second examination, Federal Government Executive Branch Perspectives, consisted of coding 74 data points from fourteen different sources (see table 6).

RUBRIC 2: EXECUTIVE BRANCH GUIDANCE PERSPECTIVES

Army Information Tasks	Sources: Homeland Security Presidential Directives (HSPD)				Other Executive Orders				Dept of Homeland Security (DHS) Guidance & Policies				Federal Emergency Management Agency (FEMA) Guidance & Policies				Quadrennial Defense Review				Army Information Capabilities
	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	
INFORMATION ENGAGEMENT																			1		Leader & Soldier Engagement
			1			1		1			3	4							1		Public Affairs
	1										2								1		Psychological Operations
			1								2								1		Combat Camera
			1			1	1				5	1							1		Strategic Communications
COMMAND AND CONTROL WARFARE																			1		Physical Attack
																			1		Electronic Attack
																			1		Electronic Warfare Support
																			1		Computer Network Attack
																			1		Computer Network Exploitation
INFORMATION PROTECTION										5	1								1		Information Assurance
		1								2	1								1		Computer Network Defense
		1								1									1		Electronic Protection
		1								3	2								1		Operations Security
		1								1	2								1		Physical Security
OPERATIONS SECURITY		1								4									1		Counter-Intelligence
MILITARY DECEPTION																			1		Military Deception
TOTAL	0	0	10	0	1	2	1	1	0	0	31	11	0	0	0	0	0	0	17	0	

TOTAL PERCENTAGES (Based on Sampling)	
1.4%	% Specifically Prohibits Use
2.7%	% Implied Prohibition of Use
79.7%	% Implied Permission of Use
16.2%	% Specified Permission of Use

TOTAL Samples: 74

NOTES:
(1) Uses terminology similar to concept definition specified in Chapter 1
(2) Uses terminology similar to concept definition specified in Chapter 1, or not language present
(3) No Pattern - less than two occurrences
(4) Pattern - Two occurrences
(5) Significant Pattern - more than three occurrences

Figure 8. Federal Executive Branch Perspectives Rubric

Source: Created by Author

Homeland Security Presidential Directives (HSPD).

The most telling directive was HSPD-8, which implied that information engagement, command and control warfare, operations security, and information protection tasks could be performed in domestic support operations. HSPD-8 specifically stated,"…Federal preparedness assistance will support State and local entities' efforts including planning, training, exercises, interoperability, and equipment acquisition for major events as well as capacity building for prevention activities such as ***information gathering, detection, deterrence,*** and collaboration related to terrorist attacks. Such assistance is not primarily intended to support existing capacity to address normal local first responder operations, but to build capacity to address major events, especially terrorism." (Department of Homeland Secuirty, 2005, p. 18).

Other Presidential Executive Orders.

Examining other executive orders yielded conflicting points regarding information engagement activities. Executive Order 12333 prohibited Peacetime PSYOP activities which "…intend to influence U.S. political process, public opinion, policies, or media…" while Department of Defense Directive S-3321 permitted, "…peacetime PSYOP consisting of planned political, economic, military and ideological activities directed towards foreign countries organizations, and individuals in order to create emotions, attitudes, understanding, beliefs, or behavior favorable to the achievement of U.S. political and military objectives." (1st Cavalry Division, 2007, App 4 - Legal, p. 1).

Department of Homeland Security Guidance and Policy.

Reviewing the 2006 Homeland Defense Strategy, we noted possible implied policy permitting counter-intelligence (an Army operations security capability): "[T]ogether with the Intelligence Community and civil authorities, DoD works to obtain and promptly exploit all actionable information needed to protect the United States." (Department of Defense, 2005, p. 2).

Quadrennial Defense Review (QDR).

Reviewing the 2006 QDR did not yield any concrete directives or guidance regarding information, operations in domestic operations. However, there was sufficient language directing the services to close capability gaps in Public Affairs, Defense Support to Public Diplomacy, Military Diplomacy and Information Operations, including Psychological Operations. Closing those gaps would be critical to achieving a seamless strategic communication organization across the U.S. Government." (Deparment of Defense, 2006, p. 92).

Table 6. Federal Executive Branch Perspective Sources Examined
1st Cavalry Division G3. Annex E (Rules of Engagement) 1ST Cavalry Division CONPLAN GARDEN PLOT, 04 September 2007.
1st Cavalry Division G3. Appendix 4 (Legal Constraints) to Annex E (Rules of Engagement) 1ST Cavalry Division CONPLAN GARDEN PLOT, 04 September 2007.
Homeland Security Council. *National Continuity Policy Implementation Plan.* Washington, DC: Government Printing Office, August 2007.
United States General Accounting Office. *Emergency Preparedness and Response, Some Issues and Challenges Associated with Major Emergency Incidents (Statement of William O. Jenkins, Director Homeland Security and Justice Issues).* Washington, DC: Government Printing Office, February 23, 2006.
--. *GAO's High Risk Program (Statement of David M. Walker, Comptroller General of the United States).* Washington, DC: Government Printing Office, March 15, 2006.
US Department of Agriculture. Interim Avian Influenza (AI) Response Plan. Washington, DC: Government Printing Office, January 2006
US Department of Defense. *Strategy for Homeland Defense and Civil Support.* Washington, DC: Government Printing Office. June 2005.
US Department of Defense. *Department of Defense Implementation Plan for Pandemic Influenza.* Washington, DC: Government Printing Office, August 2006.
US Department of Defense. *Quadrennial Defense Review Report, 2006.* Washington, DC: Government Printing Office, February 2006.
US Department of Homeland Security. *The Federal Response to Hurricane Katrina, Lessons Learned.* Washington, DC: Government Printing Office, February 2006.
US Department of Homeland Security. *Hurricane Rita DHS SITREP #6,* 22 0600 September 2005.
US Department of Homeland Security. *Interagency Integrated Standard Operating Procedure - Joint Field Office (JFO) Activation and Operations, Version 8.2.* Washington, DC: Government Printing Office. April 28, 2006.
US Department of Homeland Security. *National Preparedness Goal (Draft).* Washington, DC: Government Printing Office, December 2005.
US Department of Homeland Security. *Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources.* Washington, DC: Government Printing Office, June 21, 2006.
US House of Representatives. *The State of Homeland Security 2006.* Washington, DC: Government Printing Office, March 3, 2006.

Table 6. Federal Executive Branch Perspective Sources Examined

Source: Created by Author

Department of Defense Perspectives

The third examination, Department of Defense Perspectives, consisted of coding 181 data points from thirteen different sources (see table 7).

RUBRIC 3: DOD PERSPECTIVES

Army Information Tasks	DSCA Guidance			Joint Doctrine			Combined Doctrine			Army Doctrine			Army Information Capabilities
	Specifically Prohibits Use	Implied Prohibition of Use (1)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specifically Prohibits Use	Implied Prohibition of Use (1)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	
INFORMATION ENGAGEMENT			4			2			2			5	Leader & Soldier Engagement
			4			2			2			4	Public Affairs
	1		3			3			1			5	Psychological Operations
			3			3			1			4	Combat Camera
		1	4			3			1			5	Strategic Communications
COMMAND AND CONTROL WARFARE			2			2						2	Physical Attack
			2			3						3	Electronic Attack
			3			3						3	Electronic Warfare Support
			2			3						2	Computer Network Attack
			3			3						4	Computer Network Exploitation
INFORMATION PROTECTION			3			4	1					4	Information Assurance
			3			4						4	Computer Network Defense
			3			4						4	Electronic Protection
			3			4	1					5	Operations Security
			3			5						4	Physical Security
OPERATIONS SECURITY			3			4						4	Counter-Intelligence
MILITARY DECEPTION			3			2						3	Military Deception
TOTAL	1	1	51	0	0	54	9	0	0	0	0	65	2
	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specifically Prohibits Use	Implied Prohibition of Use (1)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use

TOTAL PERCENTAGES (Based on Sampling)	
0.5%	% Specifically Prohibits Use
0.5%	% Implied Prohibition of Use
92.9%	% Implied Permission of Use
6.0%	% Specified Permission of Use

TOTAL Sample: 183

NOTES:
(1) Uses terminology similar to concept definition specified in Chapter 1
(2) Uses terminology similar to concept definition specified in Chapter 1, or no language present
(3) Pattern - less than two occurences
(4) Pattern - three occurences
(5) Significant Pattern - more than three occurences

Figure 9. Department of Defense Perspectives

Source: Created by Author

Defense Support to Civil Authorities.

In this analysis, the most controversial topic noted is the use of psychological operations (PSYOP) against a domestic audience. Indeed, it is this natural aversion which seems by default to extend to the other Army information tasks (information engagement, command and control warfare, information protection, operations security and military deception). Clay Wilson, in his Congressional Research Service article, summarized the dilemma presented by the 'internet age' in asking how we differentiate between foreign targeted audiences and American audiences:

"DOD policy prohibits the use of PSYOP for targeting American audiences. However, while military PSYOP products are intended for foreign targeted audiences, DOD also acknowledges that the global media may pick up some of these targeted messages, and replay them back to the U.S. domestic audience. Therefore, a sharp distinction between foreign and domestic audiences cannot be maintained." (Wilson, 2007, p. 4).

The Joint Chiefs of Staffs' *Influenza Pandemic Planning Order PLANORD,* provided another example of conflicting DSCA guidance by directing the services to "…[D]etermine [the] information operations plan. Information papers and Q&amp (sic) [questions and answers]; A (sic) products should be developed beforehand, in anticipation of a PI [influenza pandemic]." (Joint Chiefs of Staff Office, PLANORD, 14 November 2005). Further conflicting DSCA guidance manifested itself in *JP 3-28, Civil Support Operations.* In the figure below, IO is viewed as an important step in the shaping phase of a civil support operation (JP 3-28, 2006, p. 77).

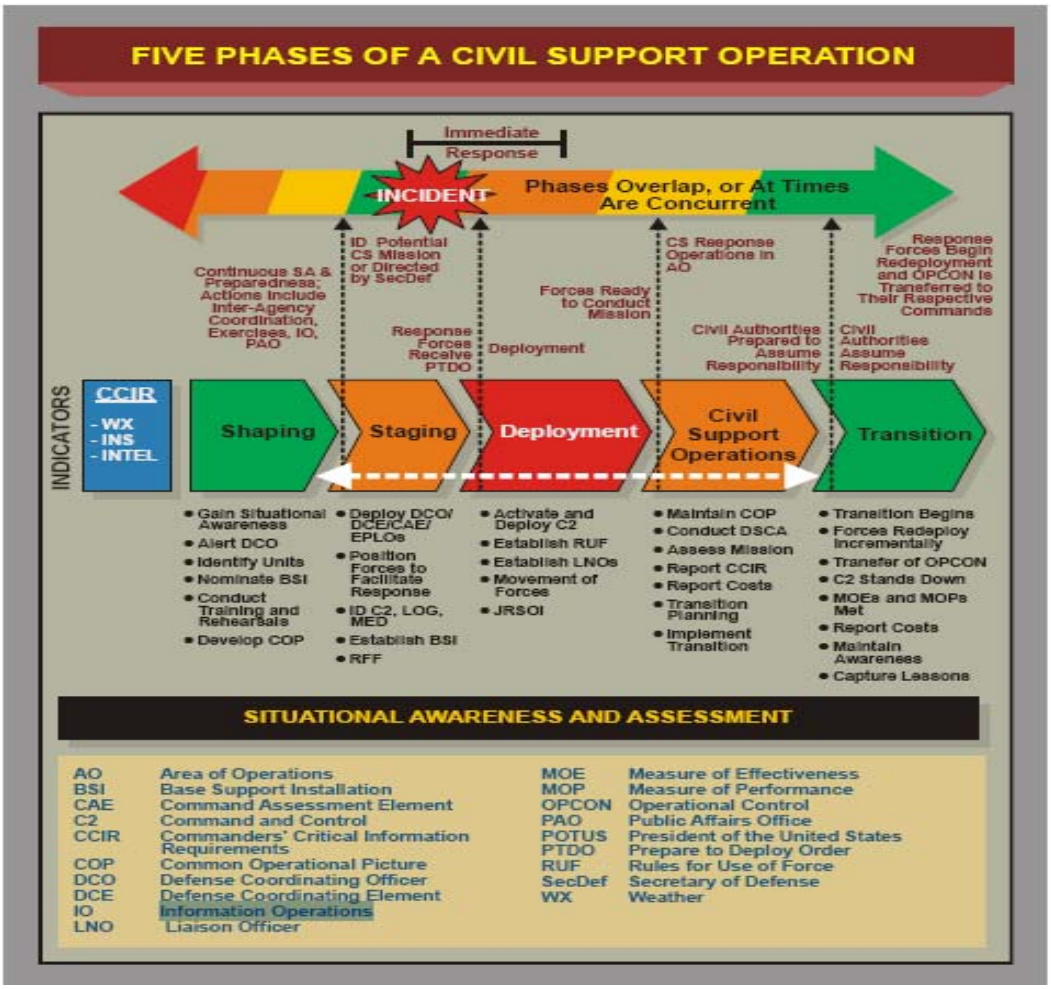

Figure 10. Five Phases of a Civil Support Operation
Source: JP 3-28, Civil Support (Figure III-V, JP 3-28, US Dept of Defense, Washington, DC, (18 December 2006), p. 76.

Joint Doctrine.

There is also inconsistency regarding 'counter-intelligence' and 'computer network operations' in *JP 3-13, Information Operations* — which implies these capabilities might be applicable in domestic operations after an operational law legal review has been completed:

"The nature of the information environment complicates compliance with legal constraints and restraints. Thus the IC [intelligence considerations in planning

information operations] must implement technical and procedural methods to ensure compliance with the law. Additionally, intelligence may be supplemented with information legally provided by law enforcement or other sources. Especially in the area of CNO, where the application of different domestic and international laws may be unclear, close coordination among the operational, legal, and law enforcement communities is essential." (JP 3-13, 2006, p. 43).

Army Doctrine.

Joint doctrine is not the only area noted for inconsistencies, Army doctrine was just as susceptible. Regarding soldiers and leaders conducting 'face-to-face' engagements with civilians, *FM 3-6, Urban Operations,* provided the following guidance (implying usage regarding domestic civil authorities):

"In an attempt to develop close relationships with the civilian populace, Army commanders may continue to work closely with traditional, informal leaders to the exclusion of the new authority. These actions, while they are often conducted out of practical and immediate necessity, may run counter to the lead agency's goal. Overall, Army commanders must nest their IO campaign objectives and themes within those of the lead agency, aggressively coordinate with other governmental agencies and coalition partners, and synchronize activities down to the tactical level to prevent working at odds and avoid information fratricide." (FM 3-06, 2005, p. 101).

Keeping Army information task capabilities 'segregated' in domestic environments was also a challenge. *FM 3-07, Stability Operations,* noted:

"The cascading effects of events and their global magnification through the media further exacerbates this characteristic of the environment. Army forces can master this

environment, in part, by gaining and maintaining information superiority through effective employment of information operations (IO)." (FM 3-07, 2003, p. 24).

This was reinforced in *FM 3-61.1, Public Affairs Tactics, Techniques, and Procedures:* "Information campaign objectives cannot be neatly divided by discipline, such as PA, CA and PSYOP. The responsible organization cannot be easily determined solely by looking at the medium, the message or the audience." (FM 3-61.1, 2000, p. 94).

Table 7. Department of Defense Perspectives Sources Examined
England, Gordon. Deputy Secretary of Defense Memorandum, Subject: "Implementation of the Strategy of Homeland Defense and Civil Support, June 24, 2005.
Joint Chiefs of Staff. *CJSC PLANORD, Influenza Pandemic*, November 14, 2005.
Joint Staff. *CJCSM 3500.04D, Universal Joint Task List (UJTL).* Washington, DC: Government Printing Office, August 1, 2005.
US Department of the Army (?). *CMOC Guide.* Fort Bragg, NC: USACAPOC (?), January 24, 2002.
US Department of the Army. *FM 3-06, Urban Operations (Final Draft).* Washington, DC: Government Printing Office, July 2005.
US Department of the Army. *FM 3-07, Stability and Support Operations.* Washington, DC: Government Printing Office, February 2003.
US Department of the Army. *FM 3-61.1, Public Affairs Tactics, Techniques, and Procedures.* Washington, DC: Government Printing Office, October, 2000.
US Department of the Army. *FM 7-15, the Army Universal Task List.* Washington, DC: Government Printing Office, August 31, 2003.
US Department of Defense. *Implementation of the National Strategy for Pandemic Influenza (Department of Defense Task Breakout) Briefing.* November 8, 2006.
US Department of Defense. *JP 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace.* Washington, DC: Government Printing Office, May 24, 2000.
US Department of Defense. *JP 3-13, Information Operations.* Washington, DC: Government Printing Office, February 13, 2006.
US Department of Defense. *Quadrennial Defense Review Report.* Washington, DC: Government Printing Office, February 6, 2006.
Wilson, Clay. "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues." In CRS Report for Congress, RL31787. Washington, DC: Congressional Research Service, June 5, 2007.

Table 7. Department of Defense Perspectives Sources Examined

Source: Created by Author

Combatant Commanders' Perspectives

The fourth examination, Combatant Commanders' (COCOM) Perspectives, consisted of coding 160 data points from twenty-one different sources (see table 8).

RUBRIC 4: COCOM PERSPECTIVES

Army Information Tasks	USIFCOM Guidance						USSTRATCOM Guidance						FORSCOM Guidance						NORTHCOM Guidance						ARNORTH Guidance						Army Information Capabilities
INFORMATION ENGAGEMENT			2																												Leader & Soldier Engagement
		2														5				1	3	7						3			Public Affairs
		2												1						3	3							2			Psychological Operations
		2												4	1						3					3					Combat Camera
		2												4						1	8					3					Strategic Communications
COMMAND AND CONTROL WARFARE			2																	2	1										Physical Attack
		2																		2	1										Electronic Attack
		2																		2	1										Electronic Warfare Support
		2																		2	1										Computer Network Attack
		2																		2	1										Computer Network Exploitation
INFORMATION PROTECTION		2												2							5					3					Information Assurance
			2											1							4										Computer Network Defense
			2											1							4										Electronic Protection
			2										1	2						1	3	5				2	1				Operations Security
			2											2						1	4	1				3					Physical Security
OPERATIONS SECURITY		2										1		1						1	5										Counter-Intelligence
MILITARY DECEPTION		2																		1	2										Military Deception
TOTAL	0	12	22	0	0	0	0	0	0	1	1	20	8	0	19	52	15	0	0	16	6										
	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use											

Sources

TOTAL PERCENTAGES (Based on Sampling)	
0.6%	% Specifically Prohibits Use
18.6%	% Implied Prohibition of Use
64.0%	% Implied Permission of Use
16.9%	% Specified Permission of Use

TOTAL Sample: 177

NOTES:
(1) Uses terminology similar to concept definition specified in Chapter 1
(2) Uses terminology similar to concept definition specified in Chapter 1, or no language present
(3) No Pattern - less than two occurences
(4) Pattern - three occurences
(5) Significant Pattern - more than three occurences

Figure 11. Combatant Commanders' Perspectives

Source: Created by Author

US Joint Forces Command (USJFCOM).

In looking for common threads from historical examples (1999 to 2008), this analysis examined COCOM responses to Hurricanes Katrina and Rita. Inconsistent application and confusion on information operations was noted in several after action review documents. The US Air Force's (NORTHCOM Air Component) experience in not adequately integrating information operations in a coherent fashion and its negative effect was evident: "Negative media coverage of state/federal response was not countered early enough with information on positive AF contributions to rescue, relief and recovery efforts. PA needs a chance to succeed in disaster response by being in the initial force module and having better tools (i.e. postured) for control and execution of strategic communications." (Chandler, 2006).

The Navy's Center for Naval Analysis also noted similar frustrations and recommended this flowchart as a way to work within the perceived information operations constraints for future events:

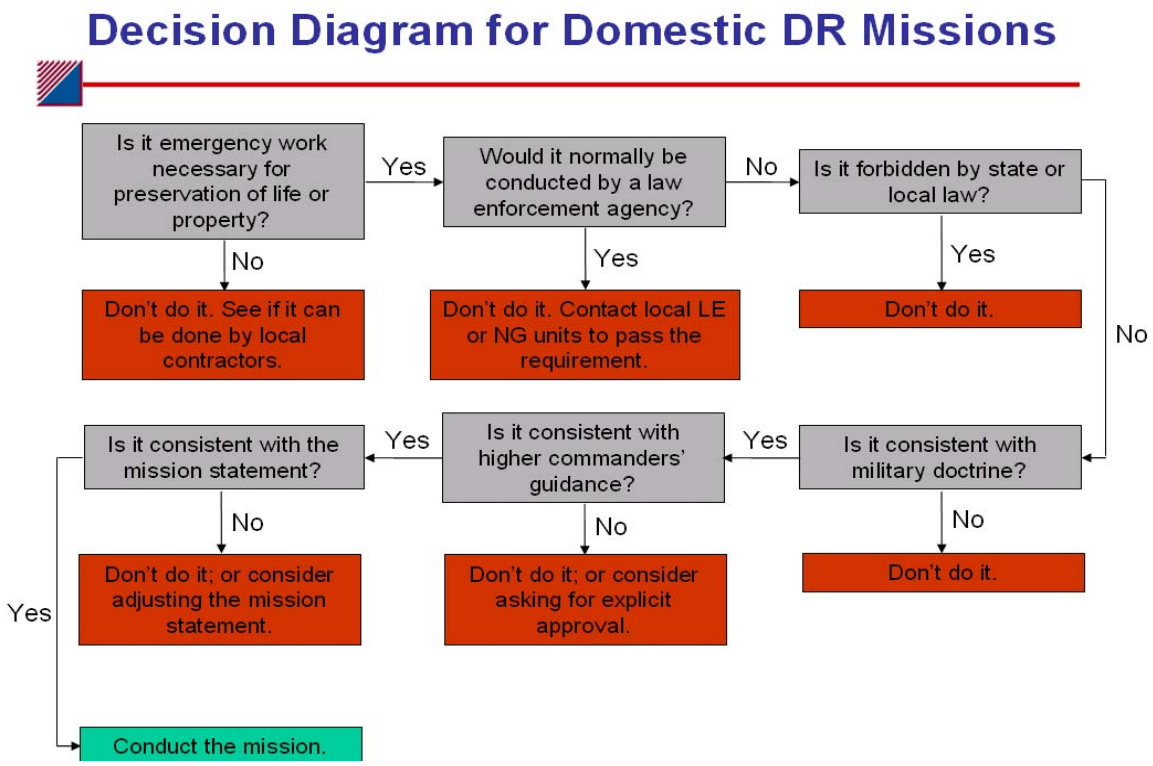

Figure 12. Decision Diagram for Domestic DR Missions
Source: CNA, *USMC Support to Hurricane Katrina: In-Progress Update* (14 December 2005)

US Northern Command (NORTHCOM).

NORTHCOM took a liberal view regarding using information operations in DSCA mission planning following Hurricane Katrina. By replacing 'PSYOP' and 'information operations' with 'public information' and 'public information teams', they appear to have 'gotten around' legal restrictions (as evidenced from this order extract):

"3.C.10.13. RECEIVE OPCON OF TACTICAL LOUDSPEAKER COMPANY PLUS WITH A C2 ELEMENT AND MOBILE PRINT CAPABILITY FROM JFCOM TO CAMP SHELBY, MS OR AS DETERMINED BY THE TACTICAL PSYOPS COMMANDER IN ACCORDANCE WITH CDR, JTF KATRINA AS SITUATION OR TASK ORGANIZATION DICTATES. ASSETS TO BE AVAILABLE FROM 5 SEPTEMBER 2005 UNTIL RELIEVED BY SECDEF, CDR USNORTHCOM, OR CDR JTF-KATRINA.

3.C.10.14. RECEIVE OPCON OF PUBLIC INFORMATION ELEMENT (FTN 30500804) FROM CDRUSSOCOM TO CAMP SHELBY OR AS DETERMINED BY THE TACTICAL PSYOPS COMMANDER IN ACCORDANCE WITH CDR, JTF KATRINA AS SITUATION OR TASK ORGANIZATION DICTATES IN ORDER TO PRODUCE PUBLIC INFORMATION MESSAGES. ASSETS TO BE AVAILABLE 5 SEPTEMBER UNTIL RELIEVED BY SECDEF, CDR USNORTHCOM OR CDR JTF-KATRINA.

3.C.10.15. RECEIVE OPCON OF AN INFORMATION PLANNING TEAM, NOT TO EXCEED TWO INDIVIDUALS (FTN 30500807) FROM CDRUSSOCOM TO PETERSON AFB,COLORADO SPRINGS TO AUGMENT NORTHCOM INFORMATION OPERATIONS. ASSETS TO BE AVAILABLE 5 SEPTEMBER UNTIL RELIEVED BY SECDEF, CDR USNORTHCOM OR CDR JTF-KATRINA.

3.C.10.16. RECEIVE OPCON OF AN INFORMATION ASSESSMENT TEAM (FTN 30500807) FROM CDRUSSOCOM TO CAMP SHELBY MS OR AS DETERMINED BY THE TACTICAL PSYOPS COMMANDER IN ACCORDANCE WITH CDR, JTF KATRINA AS SITUATION OR TASK ORGANIZATION DICTATES TO IDENTIFY INFORMATION REQUIREMENTS FOR JTF-KATRINA ASSETS TO BE AVAILABLE 5 SEPTEMBER UNTIL RELIEVED BY SECDEF, CDR USNORTHCOM OR CDR JTF-KATRINA." (NORTHCOM, September 05, 2005).

US Forces Command (FORSCOM).

Our analysis noted that FORSCOM specifically directed operations security measures regarding Hurricane Rita. NOTE: This was typical of language used during Hurricane Katrina also:

"3.D.2. IN-TRANSIT SECURITY IS A CRITICAL ASPECT OF FORCE PROTECTION PLANNING. COMMANDERS ARE REMINDED TO CONSIDER THE CURRENT THREAT AND VULNERABILITIES WHEN DEVELOPING IN-TRANSIT SECURITY PLANS TO PROTECT DEPLOYING/RE-DEPLOYING PERSONNEL AND EQUIPMENT." (FORSCOM, 2005, p. 5).

FORSCOM also encouraged information engagement tasks as evidenced by this excerpt (although it was not apparent whether a conscious effort was made to coordinate, synchronize, and de-conflict):

"PUBLIC AFFAIRS PERSONNEL AND DEPLOYED PERSONNEL ARE ENCOURAGED TO TALK ABOUT WHAT THEY ARE DOING TO ASSIST WITH THE DISASTER RELIEF WITHIN THEIR OWN KNOWLEDGE, EXPERIENCE

AND STAYING WITHIN THEIR OPERATIONAL SCOPE." (FORSCOM RITA EXORD, 23 September 2005, p. 7).

FORSCOM was also very clear in prohibiting 'deliberate' counter-intelligence from taking place, but did make provisions for dealing with 'accidental' collection:

"INFORMATION RELATED TO US PERSONS AS DEFINED IN EXECUTIVE ORDER 12333 WILL BE COLLECTED BY ARMY MILITARY INTELLIGENCE PERSONNEL PER AR 381-10. ANY FORCE PROTECTION INFORMATION WILL BE ROUTED THROUGH MILITARY POLICE CHANNELS. SOLDIERS WHO INADVERTENTLY OBTAIN FORCE PROTECTION AND/OR THREAT INFORMATION WILL CONTACT THE NEAREST CIVILIAN LAW ENFORCEMENT OFFICIAL OR THE MILITARY POLICE." (FORSCOM WARNO, September 18, 2005, p. 4).

Finally, one of the most compelling pieces of data amassed was reflected in the Army's 4th PSYOP Group organization changes as a result of 'lessons learned' following both Hurricane Katrina and Rita. These two slides illustrated the 3d PSYOP Battalion's missioning from 'general world-wide' support, to now dedicated support to NORTHCOM:

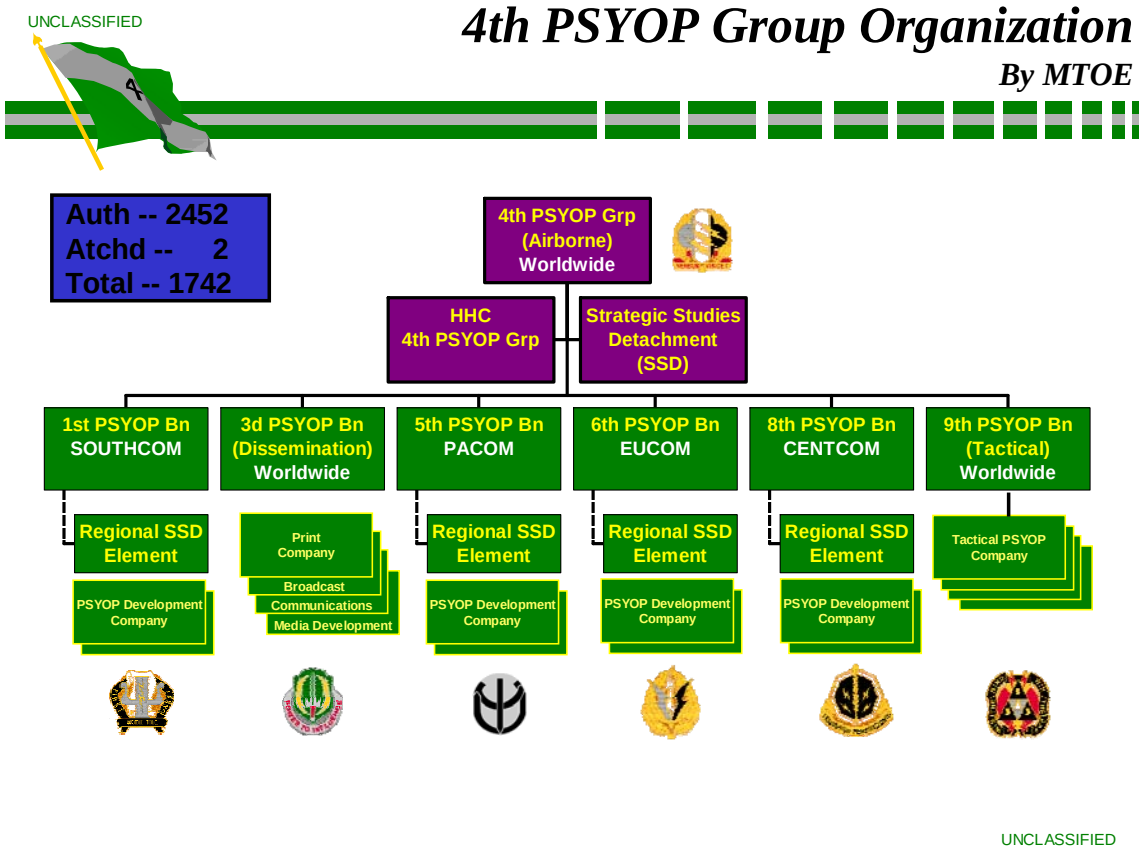

Figure 13. 4th PSYOP Group Organization Prior to August 2007.
Source: Weatherford, *9th PSYOP Information Brief* (August 2007)

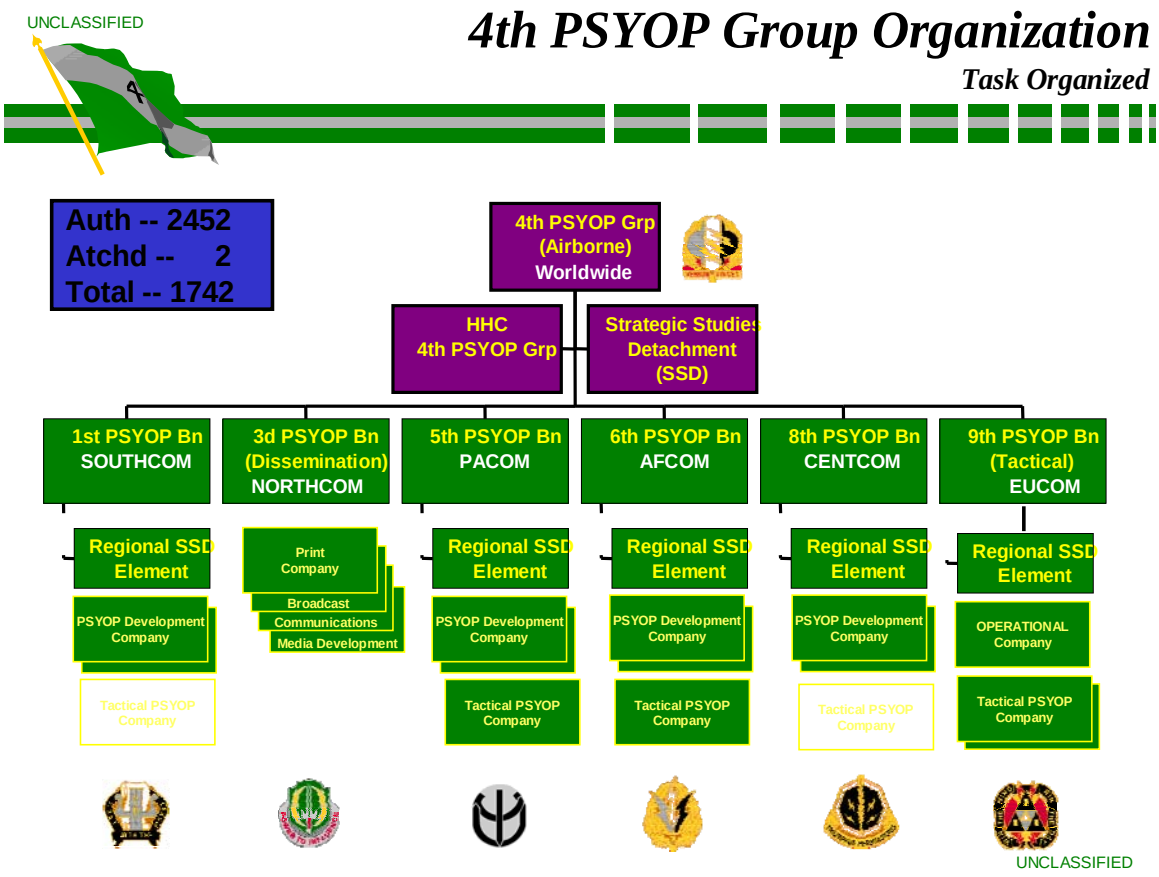

Figure 14. 4th PSYOP Group Organization After August 2007.
Source: Weatherford, *9th PSYOP Information Brief* (August 2007)

US Army Northern Command (ARNORTH).

ARNORTH was not ambiguous in its attempt to plan and conduct 'PSYOP' in support of Hurricane Katrina relief efforts as evidenced by this request for forces:

"1.A.(U) JTF-KATRINA COMMANDER REQUESTS NORTHCOM PROVIDE PSYCHOLOGICAL OPERATIONS(PSYOPS) TEAMS TO CONDUCT INFORMATION OPERATIONS. THE ABILITY TO DISTRIBUTE INFORMATION TO REFUGEES IS LIMITED WITHIN THE MOST DAMAGED AREAS OF THE JOA. IN ORDER TO FACILITATE THE DISTRIBUTION OF CRITICAL EVACUATION INSTRUCTIONS TO REMAINING PERSONNEL STRANDED WITHIN THE JOA, JTF-KATRINA IS REQUESTING PSYOPS TEAMS TO BROADCAST INFORMATION WITHIN THE JOA.//" (ARNORTH, 2005).

Table 8: Combatant Commanders' Perspectives Sources Examined
ARNORTH G3. JTF Katrina Warning Order (WARNORD), 04 0453Z SEP 05.
ARNORTH G3. JTF-Katrina Commander's Assessment Briefing, 21 1900 SEP 05.
ARNORTH G3. JTF Rita Commander's Assessment Briefing, 25 1800 CDT SEP 05.
ARNORTH G3. RFF 06 - JTF Katrina Request for Forces, 31 AUG 05.
Chandler, Howie, Lt Gen. "AF Hurricane Response and Application to WMD Attack." Briefing to Headquarters, US Air Force, 17 March 2006.
MOD 1 to CDRUSNORTHCOM EXECUTION ORDER (EXORD) for the Employment of Title 10 Forces within the JTF-KATRINA JOA to Provide Humanitarian Assistance in Support of FEMA. USNORTHCOM, 07 September 2005.
MOD 14 to CDRUSNORTHCOM EXORD for Defense Support to Civil Authorities (DSCA) in Support of FEMA Disaster Relief Operations for Hurricane Katrina. USNORTHCOM, 05 1630Z SEP 05.
MARFOR Katrina Staff. "USMC Operations in Support of Hurricane Katrina Relief." MARFOR Katrina Lessons Learned Staff Briefing, September, 2005.
McKinney, Cynthia A. *Supplementary Report to the Findings of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina,* February 6, 2006
OPNAV NOC. Hurricanes Rita and Katrina Update Brief, 24 2200Z SEP 05.
US Army Corps of Engineers (USACE). *USACE Operations Center (UOC) Update Brief,* 23 0900 September 2005.
US Department of the Navy. "USMC Support to Hurricane Katrina: In-progress Update." Center for Naval Analysis Briefing, December 14, 2005.
USCENTCOM J3. *USCENTCOM PI CONPLAN Briefing.* March 13, 2006.
USFORSCOM G3. FRAGO 18 to FORSCOM EXORD in Support of Hurricane Katrina, 13 1941Z SEP 05.
USFORSCOM G3. FORSCOM WARNORD for Tropical Storm Rita, 18 2354Z SEP 05.
USFORSCOM G3. FORSCOM WARNORD#2 for Tropical Storm Rita, 20 1254Z SEP 05.
USFORSCOM G3. FORSCOM Requirements/Orders Synchronization Matrix, 11 1808 SEP 05.
USNORTHCOM J3. Operational /DOD Support for Disaster Relief Operations EXORD, 26 1930Z AUG 05.
USNORTHCOM J3. Mod 13 to Operational /DOD Support for Disaster Relief Operations EXORD, 04 1600Z SEP 05.
USPACOM G3. *Pandemic Influenza Tabletop Exercise.* Ford Island, HI, 15-16 November 2005.
Weatherford, D.J. *9th PSYOP Information Brief.* August, 2007.

Table 8. Combatant Commander's Perspectives Sources Examined

Source: Created by Author

Department of the Army Perspectives

The fifth examination, Department of the Army Perspectives, consisted of coding only two data points from one source (see table 9). Unfortunately, the majority of relevant documents that might have yielded insights in this arena were either classified or 'For Official Use Only' and thus were outside the limitations and delimitations established in Chapter 1.

RUBRIC 5: DEPARTMENT (HQDA, USARC, NGB) PERSPECTIVES

Army Information Tasks	Sources: HQDA Guidance						USARC Guidance						NGB Guidance						Army Information Capabilities
INFORMATION ENGAGEMENT																			Leader & Soldier Engagement
																			Public Affairs
																			Psychological Operations
																			Combat Camera
																			Strategic Communications
COMMAND AND CONTROL WARFARE																			Physical Attack
																			Electronic Attack
																			Electronic Warfare Support
																			Computer Network Attack
																			Computer Network Exploitation
INFORMATION PROTECTION			1																Information Assurance
																			Computer Network Defense
																			Electronic Protection
					1														Operations Security
																			Physical Security
OPERATIONS SECURITY																			Counter-Intelligence
MILITARY DECEPTION																			Military Deception
TOTAL	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use							

TOTAL PERCENTAGES (Based on Sampling)	
0.0%	% Specifically Prohibits Use
0.0%	% Implied Prohibition of Use
50.0%	% Implied Permission of Use
50.0%	% Specified Permission of Use

TOTAL Sample: 2

NOTES:
(1) Uses terminology similar to concept definition specified in Chapter 1
(2) Uses terminology similar to concept definition specified in Chapter 1, or no language present
(3) No Pattern - less than two occurences
(4) Pattern - three occurences
(5) Significant Pattern - more than three occurences

Figure 15. Department Perspectives Rubric

Source: Created by Author

Table 9: Department Perspectives Sources Examined
US Department of the Army, US Army Corps of Engineers (USACE). *USACE Operations Center Update Brief,* 23 0900 September 2005.

Table 9. Department Perspectives Sources Examined

Source: Created by Author

Academic and Civilian Perspectives

The final area examined, Academic and Civilian Perspectives, consisted of coding 70 data points from sixteen different sources (see table 10).

RUBRIC 6: ACADEMIA & CIV PERSPECTIVES

Army Information Tasks:	Sources																						Army Information Capabilities
	Terms of Reference				Propaganda Issues				Legal Issues				Homeland Security & Defense Issues										
INFORMATION ENGAGEMENT			2				3	1			1	1				3							Leader & Soldier Engagement
			2				3	1				1				2							Public Affairs
	1					2	4			1	1												Psychological Operations
			1				1				1					2							Combat Camera
			2				5					1				2							Strategic Communications
COMMAND AND CONTROL WARFARE									1														Physical Attack
									1	1													Electronic Attack
									1	1													Electronic Warfare Support
									1	1													Computer Network Attack
									1	1						1							Computer Network Exploitation
INFORMATION PROTECTION										1						1							Information Assurance
										1						1							Computer Network Defense
										1						1							Electronic Protection
							1			1						1							Operations Security
										1						1							Physical Security
OPERATIONS SECURITY									1	1						1							Counter-Intelligence
MILITARY DECEPTION									1	1						1							Military Deception
TOTAL	0	1	7	0	0	2	17	2	9	15	1		0	0	17	0							
	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use	Specifically Prohibits Use	Implied Prohibition of Use (1)	Implied Permission of Use (2)	Specified Permission of Use							

TOTAL PERCENTAGES (Based on Sampling)	
0.0%	% Specifically Prohibits Use
16.9%	% Implied Prohibition of Use
78.9%	% Implied Permission of Use
4.2%	% Specified Permission of Use

TOTAL Sample: 71

NOTES:
(1) Uses terminology similar to concept definition specified in Chapter 1
(2) Uses terminology similar to concept definition specified in Chapter 1, or no language present
(3) No Pattern - less than two occurences
(4) Pattern - three occurences
(5) Significant Pattern - more than three occurences

Figure 16. Academic & Civilian Perspectives Rubric

Source: Created by Author

Terms of Reference.

The analysis revealed that there was a lot of controversy surrounding the Smith - Mundt Act of 1948, which prohibits psychological operations against domestic audiences. Bryan Hill's essay succinctly summarized the confusion over this issue: "Although it applies only to the State Department, many government lawyers and public affairs officers stretched the law beyond its original intent and have used it to hamstring American public diplomacy and political warfare for decades. Until the SMA [Smith-Mundt Act], and our understanding of it, is updated, U.S. public diplomats, political warriors, and information operations specialists will lack the tools they need to combat the ideologies of our extremist enemies. And we will all be less safe because of it." (Hill, 2007, p. 1).

Propaganda Issues.

According to this analysis, the term propaganda was also another source of controversy. Despite the differing opinions regarding the Smith -Mundt Act, Todd Schmidt pointed out in his essay that the challenge in today's global interconnected environment was that the US Government needs to consider the US domestic population as a 'target audience'. (Schmidt, 2007, p. 5). W.C. Garrision pointed out the advantages information engagement capabilities have in countering rumors and disinformation in domestic operations:

"A counter-propaganda effort can get needed information to displaced populations and combatants. Victims in a dysfunctional society can use reliable counter-propaganda information to locate relief sites." (Garrison, 1999, p. 8).

Legal Issues.

Legal issues were another area of controversy. Thomas Wingfield and James Michael summarized the issue regarding computer network defense and information assurance capabilities. Are intrusions an act of war or a criminal act: "[T]he legal challenge [of Posse Comitatus] in any computer intrusion is properly characterizing the intruders' categorical legal identity." (Wingfield, 2004, p. 2).

Ollie Washington, Jr. clearly described the problem in his essay: "Domestically, the privacy and search and seizure laws of the U.S. significantly impair the ability of the government and military to actively pursue hackers, terrorists and spies. While I would not propose the mass abdication of individual rights, I feel that the elements of the U.S. government should work with the Department of Justice and the Congress to find ways to bring applicable laws into better synchronization with the high technology systems that exist now and into the future." (Washington, 2001, p. 12).

Homeland Security and Defense Issues

Preparation for a future pandemic disease outbreak was another area of concern according to this analysis. The Department of Health and Human Services identified the critical point: "Dissemination of information to all Americans is a critical component of effective pandemic planning and response." (US Department of Health and Human Services, 2005, p. 9).

Table 10: Academic and Civilian Perspectives Sources Examined
Center for Strategic and International Studies, Homeland Security Program. *Model Operational Guidelines for Disease Exposure Control (Pre-Publication Draft).* Washington, DC: Center for Strategic Studies, November 2, 2005.
Clarke, Richard A. *LNG Facilities in Urban Areas.* Arlington, VA: Good Harbor Consulting, LLC, May, 2005.
Dietz, Lawrence D. *Information Operations (IO) 2006: a Critical Assessment of IO and The NATO Alliance.* Cuptertino, CA: Symantec Corporation, October, 2006.
Dhillon, Joginder S. and Robert I Smith. "Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques." June 12, 2001.
Garrison, W.C. *Information Operations and Counter-propaganda: Making a Weapon of Public Affairs.* Carlisle Barracks, PA: US Army War College, March 17, 1999.
Gough, Susan L. *The Evolution of Strategic Influence.* Carlisle Barracks, PA: US Army War College, January 30, 2004.
Healy, Gene. "Deployed in the U.S.A. , the Creeping Militarization of the Home Front" in *Policy Analysis, No 503,* December, 17, 2003.
Hill, Bryan. "The Smith-Mundt Act of 1948: Comments, Critiques, and the way Forward." In *The Center for Security Policy, Occasional Papers Series*, no. 20 April, 2007.
Martemucci, Matteo, G. *Regaining the High Ground: the Challenges of Perception Management in National Strategy and Military Operations.* Washington, DC: Joint Forces Staff College, June `7, 2007.
The Role of Information Operations Campaigns in Shaping a Political Reality: The American Experience as an Example. January 11, 2007.
Rohm, Fredric W, Jr. "Merging IO and PSYOP." January 11, 2007.
Schmidt, Todd. "The Global Information Environment and 21st Century Warfare: Targeting Public Opinion in the 5th Dimension." January 11, 2007.
US Department of Health and Human Services. *HHS Pandemic Influenza Plan.* Washington, DC: Government Printing Office, November, 2005.
US Department of State. *US International Implementation Strategy on Avian Influenza (Draft).* Washington, DC: Government Printing Office, August 17, 2005.
Washington, Ollie, Jr. *The Legal and Ethical Implications of Information Operations.* Carlisle Barracks, PA: US Army War College, April 10, 2001.
Wingfield, Thomas C. and James B. Michael. *An Introduction to Legal Aspects of Operations in Cyberspace.* Monterey, CA: Naval Post Graduate School, April 28, 2004.

Table 10. Academic and Civilian Perspectives Sources Examined

Source: Created by Author

Summary

This analysis examined numerous sources of data in an attempt to capture the collective thought across the 'information operations community' regarding the use of information as an element of combat power in domestic support operations. Chapter Five will summarize our conclusions regarding the 'collective' thought on overcoming legal limitations for using Army information tasks in domestic operations.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Chapter one of this thesis stated that information is an element of combat power that commanders and staffs must integrate into the concept of operations through the operations process spelled out in FM 3-0, Operations. Since the 1990's, US Army has used information with varying degrees of success to influence the outcome of military operations. It has moved from using information as a methodology of attacking an enemy's command, control, and communications systems to a concept of integrated tools a commander may employ to inform or influence local and regional audiences in favor military operations.

Chapter two's literature review indicated there was adequate depth and breadth to proceed with analysis and attempt to answer the original thesis question: Can information tasks (information engagement, command and control warfare, military deception, information protection, and operations security) be legally applied in domestic operations? Chapter three's research methodology permitted exploration and analysis framed around three focus areas:

- Legal restrictions for planning, preparing, executing and assessing the effectiveness of Army information tasks (information protection, military deception, operations security, command and control warfare, and information engagement) in domestic support operations.
- Common threads (or insights) from recent history (1999 to the present) that could be applied to future domestic operations.

- Parallels between operational historical examples (domestic operations and overseas stability operations).

This chapter presents findings regarding whether Army information tasks can be legally and doctrinally applied in domestic operations. By examining each Army information task in light of the content analysis methodology, it was possible to provide answers regarding the collective community thoughts, or perspectives, as to whether or not it is possible to apply these tasks in domestic operations.

Information Tasks in Domestic Operations.

The examination of findings regarding Army information tasks in domestic operations was startling. The findings indicate the collective thought (or opinion) of the 'Information Community' is that it ***may be possible to apply Army information tasks legally in domestic operations.*** This table summarizes the findings in the six areas examined (Legislation, Executive Branch, Department of Defense, Combatant Commander, Department of the Army, and Department of Defense, Combatant Commander, Department of the Army, and Academic/Civilian Perspectives):

Table 11. Army Information Operation Tasks						
	Legislative	**Executive Branch**	**Department of Defense**	**Combatant Commander**	**Department of the Army**	**Academic / Civilian**
Percentage Specifically Prohibit Use	0%	1.4%	0.5%	0.6%	0%	0%
Percentage Implied Prohibition	0%	2.7%	0.5%	18.6%	0%	16.9%
Percentage Implied Usage	53.3%	79.7%	92.9%	64%	50%	78.9%
Percentage Specified Permission Usage	1.9%	16.2%	6%	16.9%	50%	4.2%

Table 11. Army Information Operations Tasks

Source: Created by Author

The majority opinion across all six perspectives points to an 'implied' permission for using information tasks in domestic operations. This language is consistent with FM 3-0 and seems to validate FM 3-0' authors. ***Therefore it must be concluded that Army Information Tasks may be legally and doctrinally applied in domestic operations.***

Does this mean these tasks can be applied fully; e.g. utilizing all the capabilities associated with a given Army information task? Here is where ***there is some differing opinions regarding whether 'all', 'some' or 'none' of these Army information task capabilities may be utilized in domestic operations.*** The following discussion presents conclusions regarding the application of each information task capability in domestic operations.

Information Engagement Capabilities Application.

"Information Engagement" and its associated capabilities were examined first. They included: Leader and Soldier Engagement, Public Affairs, Psychological Operations, Combat Camera, and Strategic Engagement. It is apparent that Leader and Soldier Engagement, along with Strategic Communications appear to be the most widely accepted Information Engagement capabilities for use in domestic operations. This Table summarizes the findings for all six perspectives:

Table 12. Information Engagement Capabilities

	Instances Specifically Prohibit Use	**Instances Implied Prohibit Use**	**Instances Implied Usage**	**Instances Specified Permission Usage**
Leader & Soldier Engagement	0	1	43	8
Public Affairs	0	0	35	26
Psychological Operations	1	2	35	3
Combat Camera	0	0	41	3
Strategic Communications	0	3	56	0

Table 12. Information Engagement Capabilities

Source: Created by Author

Psychological Operations remains a strong point of contention, even though this data would suggest some level of acceptance in domestic operations. On the one hand, the Smith - Mundt Act implies prohibition of psychological operations against a domestic audience; on the other hand, the 4th PSYOP Group has made a conscious effort to support psychological operations against a domestic audience by realigning its third

battalion from 'general support' to 'direct support' for NORTHCOM. Indeed, one expert summed it best regarding psychological operations and the domestic audience:

"How strongly will U.S. military PSYOP be used to manipulate public opinion, or reduce opposition to unpopular decisions in the future? … [A]nother emerging issue may be whether DOD is legislatively authorized to engage in PSYOP that may also affect domestic audiences…the DOD Information Operations Roadmap, published October 2003, states that PSYOP messages intended for foreign audiences increasingly are consumed by the U.S. domestic audience, usually because they can be re-broadcast through the global media. The Roadmap document states that, '...the distinction between foreign and domestic audiences becomes more a question of USG (U.S. Government) intent rather than information dissemination practices (by DOD)." (Wilson, 2007, pp. 15-16).

Command and Control Warfare Capabilities Application.

"Command and Control Warfare" and its associated capabilities (Physical Attack, Electronic Attack, Electronic Warfare Support, Computer Network Attack, and Computer Network Exploitation) are addressed next. The collective opinion leans towards the implied usage of all capabilities, with a higher emphasis on computer network attack capabilities. This Table summarizes findings for all six perspectives:

Table 13. Command and Control Warfare Capabilities				
	Instances Specifically Prohibit Use	**Instances Implied Prohibit Use**	**Instances Implied Usage**	**Instances Specified Permission Usage**
Physical Attack	0	3	15	0
Electronic Attack	0	4	17	0
Electronic Warfare Support	0	5	19	0
Computer Network Attack	0	3	24	0
Computer Network Exploitation	0	5	19	0

Table 13. Command and Control Warfare Capabilities

Source: Created by Author

This is an area of contention especially when considering whether or not cyber attacks are truly an 'act of war' versus 'criminal activity'. Until a firm determination can be made as to whether or not computer network attack falls under the international laws of warfare, there will be reluctance to use it in a domestic environment.

Another aspect to consider is who would be considered a 'lawful combatant' in 'cyber warfare'? One expert put it: "Since most intrusion attempts directed against the NlI/DII [national information infrastructure/defense information infrastructure] will involve innocent intermediate computer systems, Congress should be more explicit in whether, and to what extent the military may become involved in such activity. This clarification will be particularly necessary as the role and responsibility of the DOD in performing "Homeland Defense" receives greater attention." (Dhillon, 2001, p. 40).

Information Protection Capablities Application.

"Information Protection" (Information Assurance, Computer Network Defense, and Electronic Protection) and its associated capabilities were addressed next. The collective opinion points to implied usage permission in domestic operations, possibly because all these capabilities are passive in nature, and reflect 'best practices' used by both government and private industry. This Table summarizes findings for all six perspectives:

Table 14. Information Protection Capabilities				
	Instances Specifically Prohibit Use	**Instances Implied Prohibit Use**	**Instances Implied Usage**	**Instances Specified Permission Usage**
Information Assurance	0	2	41	1
Computer Network Defense	0	0	33	0
Electronic Protection	0	0	32	0

Table 14. Information Protection Capablities

Source: Created by Author

One could make the argument that since all these capabilities are passive in nature, then collective opinion should indicate and encourage their use in domestic operations.

Operations Security Capabilities Application.

"Operations Security" and its associated capabilities (Operations Security, Physical Security, and Counter-intelligence) were examined next. The data points to an implied collective opinion supporting the use of both operations security and physical

security in domestic operations. Like information assurance capabilities, these two are more passive in nature and reflect a mindset in protecting indicators and assets from exploitation. This Table summarizes findings for all six perspectives:

Table 15. Operations Security Capabilities				
	Instances Specifically Prohibit Use	**Instances Implied Prohibit Use**	**Instances Implied Usage**	**Instances Specified Permission Usage**
Operations Security	0	2	39	10
Physical Security	0	0	36	3
Counter-Intelligence	1	4	34	0

Table 15. Operations Security Capabilities

Source: Created by Author

While the collective opinion also proposes implied support for the use of counter-intelligence in domestic operations, it still remains a 'hot button' for most experts, but with careful consideration of the limitations imposed by Posse Comitatus, it may still be possible to ensure a more holistic approach to integrating these three capabilities in domestic operations. This was reflected by language in the Homeland Security Council's August 2007 National Continuity Policy Implementation Plan: "In order to ensure the safety and success of continuity operations, an effective security strategy must address personnel, physical, and information security." (Homeland Security Council, 2007, p. 5).

Military Deception Capability Application.

The final area of examination concerned "Military Deception." Surprisingly, the data pointed to a collective opinion of implied permission for use in domestic operations.

Numerous examples exist where civilian law enforcement organizations employed 'sting' operations in an attempt to lure criminals and criminal organizations to expose themselves in order to be apprehended and brought to justice. However, care must be taken when considering who or what is the deception target and the desired effect. Failure to do so could result in "information fratricide," a condition resulting from the failure of "…employing information operations elements in a way that causes effects in the information environment that impede the conduct of friendly operations or adversely effect friendly forces." (FM 3-13, 2004, p. 288). This Table summarizes findings for all six perspectives:

Table 5-6. Military Deception Capability

	Instances Specifically Prohibit Use	**Instances Implied Prohibit Use**	**Instances Implied Usage**	**Instances Specified Permission Usage**
Military Deception	0	5	18	0

Table 16. Military Deception Capability

Source: Created by Author

Recommendations

What to consider next? After having seen these conclusions and the analysis behind it, it is the considered opinion of the 'information community' that Army information tasks could and should be used in domestic operations. The scope and extent to which Army information task capabilities should be employed still remains to be studied. There are still significant issues that need resolution before Army information

tasks and associated capabilities can be confidently and fully integrated into domestic operations.

General Recommendations

- The Smith - Mundt Act: As originally drafted, it did not address prohibitions for conducting and using 'Information Engagement' assets. A thorough review of this act in light of our current 'information age' should be conducted and the Act needs to be amended accordingly in order to clarify which Army information task capabilities may or may not be applied under this act.
- The Stafford Act: It has been interpreted to give 'leeway' in using Army information tasks in domestic support operations. There is precedent in the form of specific guidance from NORTHCOM as well as FM 3-0. The Army needs to consider domestic operations and how information will be applied in those kinds of operations in the next re-write of FM 3-13, Information.

Information Engagement Capabilities Recomendations

- Psychological Operations Definition: This term has negative connotations and does not address full spectrum operations, especially when considering domestic audiences. Develop alternate terminology to Psychological Operations or even discarding the current term may be a solution. The term Strategic Communications already exists, perhaps there is merit in discarding psychological operations and replacing it with 'Operational Communications' and 'Tactical Communications'.
- Operational Communications (Proposed Definition): Focused efforts to understand and engage key regional audiences (friendly, neutral, and adversarial) in order

to create, strengthen or preserve conditions enabling the completion of the commander's end-state through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of combat power. The purpose of operational communications is to induce or reinforce regional attitudes and behavior favorable to the commander's objectives.

- Tactical Communications (Proposed Definition): Focused efforts to understand and engage key local audiences (friendly, neutral, and adversarial) in order to create, strengthen or preserve conditions enabling the completion of the commander's end-state through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of combat power. The purpose of tactical communications is to induce or reinforce local attitudes and behavior favorable to the commander's objectives.

Command and Control Capabilities Recommendations

- Lawful Combatants and Criminal Activity Clarity: The Department of Defense, in coordination with the Department of Justice, must undertake a study to clarify whether or not computer network attack is once and for all truly an act of war versus a criminal acitivity. Once this is resolved, then distinction must be made as to whether or not individuals who conduct computer network attack are truly lawful combatants or criminals. There are parallels to aspects of what constitutes terrorism and terrorists that may provide insight into resolving this issue.

Information Protection Capabilities Recommendations

- Information Protection Measures: Current best practices regarding Army

Information Protection Capabilities are already being practiced in both the civilian and military sectors. The new FM 3-28, Civil Support, under development should include language that emphasizes incorporation of information protection measures in order to ensure roles, responsibilities, planning, and implementation are understood.

Operations Security Capabilities Recommendation

- Clarity on Counter-Intelligence: The new FM 3-28, Civil Support, needs to address what constitutes counter-intelligence activities in domestic operations. Changing terminology to reflect full spectrum operations, including domestic operations may provide clarity.

- Counter-Information Surveillance (Proposed Definition): Information gathered and activities conducted to protect against espionage, adversarial information gathering activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign and domestic organizations, or foreign and domestic persons, or international and domestic terrorist activities.

Military Deception Capability Recommendation

- The Posse Comitatus Act addresses using military forces in support of law enforcement. Information Engagement, elements of Command and Control Warfare, Information Protection, and Operations Security are tasks that are not necessarily prohibited by posse comitatus. Further study is warranted to address whether or not Military Deception is or is not considered a 'law enforcement activity'. Until then, there will be reluctance to apply it to domestic operations.

Summary

The examination and debate of whether or not Army information tasks may legally and doctrinally applied in domestic operations is by no means complete. This thesis is only the first step in fully coming to terms with utilizing information as an element of combat power in domestic operations. Most of the recommendations proposed will require unified interagency action and effort in order to ensure this issue can be fully resolved.

Despite this, most of the recommendations in this thesis can be implemented in a timely fashion, since they focus on mostly doctrinal changes. Once firmly entrenched in doctrine, it will then be easier for commanders and staffs to ensure information truly is an element of combat power, fully integrated in domestic operations.

GLOSSARY

Civil Affairs (CA): Designated Active and Reserve Component forces and units organized, trained, and equipped specifically to conduct civil affairs activities and to support civil-military operations. (FM 1-02, p.1-30)

Civil Affairs Activities: Activities performed or supported by civil affairs units that (1) enhance the relationship between military forces and civil authorities in areas where military forces are present; and (2) involve application of civil affairs functional specialty skills in areas that are normally the responsibility of civil government, to enhance conduct of civil-military operations. (FM 1-02, p. 1-30)

Counter-Intelligence: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (FM 1-02, p. 1-47)

Population and Resource Control (PRC): Operations in populace and resource control (PRC) provide security for the populace, deny personnel and materiel to the enemy, mobilize population and materiel resources, and detect and reduce the effectiveness of enemy agents. Populace control measures include curfews, movement restrictions, travel permits, registration cards, and resettlement of villagers. Resource control measures include licensing, regulations or guidelines, checkpoints (for example, road blocks), ration controls, amnesty programs, and inspection of facilities. Most military operations employ some type of PRC measures. (FM 1-02, pp. 1-147 to 1-148)

Domestic Exigencies: Emergencies affecting the public welfare and occurring within the 50 states, District of Columbia, Commonwealth of Puerto Rico, US possessions and territories, or any political subdivision thereof, as a result of enemy attack, insurrection, civil disturbances, earthquake, fire, flood, or other public disasters, or equivalent emergencies that endanger life and property or disrupt the usual process of government. The term domestic emergency includes any or all of the emergency conditions defined below:

a. Civil defense emergency—A domestic emergency disaster situation resulting from devastation created by an enemy attack and requiring emergency operations during and following that attack. It may be proclaimed by appropriate authority in anticipation of an attack.

b. Civil disturbances—Riots, acts of violence, insurrections, unlawful obstructions or assemblages, or other disorders prejudicial to public law and order. The term civil disturbance includes all domestic conditions requiring or likely to require the use of Federal Armed Forces pursuant to the provisions of Chapter 15 of Title 10, United States Code.

c. Major disaster—Any flood, fire, hurricane, tornado, earthquake, or other catastrophe which, in the determination of the President, is or threatens to be of sufficient severity and magnitude to warrant disaster assistance by the federal Government under Public Law 606, 91st Congress (42 United States Code 58) to supplement the efforts and available resources of State and local governments in alleviating the damage, hardship, or suffering caused thereby.

d. Natural disaster—All domestic emergencies except those created as a result of enemy attack or civil disturbance. (FM 1-02, p. 1-65)

Information Superiority (IS): The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (FM 1-02, p. 1-100)

Information Operations Vulnerabilities: Deficiencies in protective measures that may allow an adversary to use information operations capabilities against friendly information systems or command and control systems. (FM 1-02, p. 1-99)

REFERENCE LIST

Books

Berg, Bruce L. *Qualitative Research Methods for the Social Sciences.* Boston, MA: Pearson, 2007.

Nagl, John A. *Learning to Eat Soup with a Knife, Counterinsurgency Lessons from Malaya and Vietnam.* Chicago, IL: The University of Chicago Press, 2002.

Wright, Donald P. and Colonel Timothy R. Reese. "Fighting for the Battle of Ideas in Iraq" In *On Point II: Transition to the New Campaign.* Fort Leavenworth, KS: Combat Studies Institute Press, USACAC, June 2008.

Periodicals

Bazan, Elizabeth. *Robert T. Stafford Disaster Relief and Emergency Assistance Act: Legal Requirements for Federal and State Roles in Declarations of an Emergency or Major Disaster*. Washington, DC: Congressional Research Service, September 16, 2005.

Bea, Keith. *Federal Stafford Act Assistance: Presidential Declarations, Eligible Activities, and Funding.* Washington, DC: Congressional Research Service, September 27, 2005.

Best, Richard A. and Jennifer K. Elsea. "Satellite Surveillance: Domestic Issues" in *CRS Report for Congress, RL34421*. Washington, DC: Congressional Research Service, March 21, 2008.

Bowman, Steve. *Hurricane Katrina: DOD Disaster Response.* Washington, DC: Congressional Research Service, Updated October 6, 2005.

Bowman, Steve, Lawrence Kapp, and Amy Belasco. *Hurricane Katrina: DOD Disaster Response.* Washington, DC: Congressional Research Service, September 19, 2005.

Bowman, Steve and Scott Shepard. *Homeland Security: Establishment and Implementation of the United States Northern Command.* Washington, DC: Congressional Research Service, September 8, 2005.

Elsea, Jennifer K. *The Use of Federal Troops for Disaster Assistance: Some Legal Issues.* Washington, DC: Congressional Research Service, September 16, 2005.

Healy, Gene. "Deployed in the U.S.A., the Creeping Militarization of the Home Front" in *Policy Analysis, No 503,* December, 17, 2003.

Hill, Bryan. "The Smith-Mundt Act of 1948: Comments, Critiques, and the way Forward." In *The Center for Security Policy, Occasional Papers Series,* no. 20 April, 2007.

Moore, Linda K. *Public Safety Communications: Policy, Proposals, Legislation and Progress.* Washington, DC: Congressional Research Service, August 31, 2005.

Wilson, Clay. "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues." In CRS Report for Congress, RL31787. Washington, DC: Congressional Research Service, June 5, 2007.

Government Documents

Center for Strategic and International Studies, Homeland Security Program. *Model Operational Guidelines for Disease Exposure Control (Pre-Publication Draft).* Washington, DC: Center for Strategic Studies, November 2, 2005.

Dhillon, Joginder S. and Robert I Smith. "Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques." June 12, 2001.

Homeland Security Council. *National Strategy for Pandemic Influenza Implementation Plan.* Washington, DC: Government Printing Office, May 2006.

Homeland Security Council. *National Continuity Policy Implementation Plan.* Washington, DC: Government Printing Office, August 2007.

Martemucci, Matteo, G. *Regaining the High Ground: the Challenges of Perception Management in National Strategy and Military Operations*. Washington, DC: Joint Forces Staff College, June `7, 2007.

McKinney, Cynthia A. *Supplementary Report to the Findings of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina,* February 6, 2006.

MOD 14 to CDRUSNORTHCOM EXORD for Defense Support to Civil Authorities (DSCA) in Support of FEMA Disaster Relief Operations for Hurricane Katrina. USNORTHCOM, 05 1630Z SEP 05.

Schmidt, Todd. "The Global Information Environment and 21st Century Warfare: Targeting Public Opinion in the 5th Dimension." January 11, 2007.

United States General Accounting Office. *Emergency Preparedness and Response, Some*

Issues and Challenges Associated with Major Emergency Incidents (Statement of William O. Jenkins, Director Homeland Security and Justice Issues). Washington, DC: Government Printing Office, February 23, 2006.

--. *GAO's High Risk Program (Statement of David M. Walker, Comptroller General of the United States).* Washington, DC: Government Printing Office, March 15, 2006.

US Department of Agriculture. *Interim Avian Influenza (AI) Response Plan.* Washington, DC: Government Printing Office, January 2006

US Department of the Army. *2003 Army Modernization Plan.* Washington, DC: Government Printing Office, February 2003.

US Department of the Army. *FM 1-02, Operational Terms and Graphics.* Washington, DC: Government Printing Office. September 2004

US Department of the Army. *FM 3-0, Operations.* Washington, DC: Government Printing Office. February, 2008.

US Department of the Army. *FM 3-06, Urban Operations (Final Draft).* Washington, DC: Government Printing Office, July 2005.

US Department of the Army. *FM 3-07, Stability and Support Operations.* Washington, DC:Government Printing Office, February 2003.

US Department of the Army. *FM 3-13, Information Operations.* Washington, DC: Government Printing Office. September 2004.

US Department of Defense. *Department of Defense Implementation Plan for Pandemic Influenza.* Washington, DC: Government Printing Office, August 2006.

US Department of Defense. *JP 3-13, Information Operations.* Washington, DC: Government Printing Office. February 2006.

US Department of Defense. *JP 3-28, Civil Support (Final Coordination).* Washington, DC: Government Printing Office. 18 December 2006.

US Department of Defense. *Quadrennial Defense Review Report, 2006.* Washington, DC: Government Printing Office, February 2006.

US Department of Defense. *Strategy for Homeland Defense and Civil Support.* Washington, DC: Government Printing Office. June 2005.

US Department of Health and Human Services. *HHS Pandemic Influenza Plan.* Washington, DC: Government Printing Office, November, 2005.

US Department of Homeland Security. *The Federal Response to Hurricane Katrina, Lessons Learned.* Washington, DC: Government Printing Office, February 2006.

US Department of Homeland Security. *Interagency Integrated Standard Operating Procedure - Joint Field Office (JFO) Activation and Operations, Version 8.2.* Washington, DC: Government Printing Office. April 28, 2006.

US Department of Homeland Security. *National Preparedness Goal (Draft).* Washington, DC: Government Printing Office, December 2005.

US Department of Homeland Security. *Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources.* Washington, DC: Government Printing Office, June 21, 2006.

US Department of Homeland Security, Office of the Inspector General. *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina.* Washington, DC: Government Printing Office, March 2006.

US Department of the Navy. "USMC Support to Hurricane Katrina: In-progress Update." Center for Naval Analysis Briefing, December 14, 2005.

US Department of State. *US International Implementation Strategy on Avian Influenza (Draft).* Washington, DC: Government Printing Office, August 17, 2005.

US House of Representatives. *The State of Homeland Security 2006.* Washington, DC: Government Printing Office, March 3, 2006.

Other Sources

1st Cavalry Division G3. Annex E (Rules of Engagement) 1ST Cavalry Division CONPLAN GARDEN PLOT, 04 September 2007.

1st Cavalry Division G3. Appendix 4 (Legal Constraints) to Annex E (Rules of Engagement) 1ST Cavalry Division CONPLAN GARDEN PLOT, 04 September 2007.

ARNORTH G3. JTF-Katrina Commander's Assessment Briefing, 21 1900 SEP 05.

ARNORTH G3. JTF Katrina Warning Order (WARNORD), 04 0453Z SEP 05.

ARNORTH G3. RFF 06 - JTF Katrina Request for Forces, 31 AUG 05.

ARNORTH G3. JTF Rita Commander's Assessment Briefing, 25 1800 CDT SEP 05.

Chandler, Howie, Lt Gen. "AF Hurricane Response and Application to WMD Attack."

Briefing to Headquarters, US Air Force, 17 March 2006.

Clarke, Richard A. *LNG Facilities in Urban Areas.* Arlington, VA: Good Harbor Consulting, LLC, May, 2005.

Dietz, Lawrence D. *Information Operations (IO) 2006: a Critical Assessment of IO and the NATO Alliance.* Cuptertino, CA: Symantec Corporation, October, 2006.

England, Gordon. Deputy Secretary of Defense Memorandum, Subject: "Implementation of the Strategy of Homeland Defense and Civil Support, June 24, 2005.

Federation of American Scientists. "Chapter 1 Concept and Principles" in FM 100-19, Domestic Support Operations. Washington, DC: Government Printing Office, 01 July 1993. http://www.fas.org/irp/doddir/army/fm100-19/fm100_19toc.html (Accessed November 1, 2008).

Garrison, W.C. *Information Operations and Counter-propaganda: Making a Weapon of Public Affairs.* Carlisle Barracks, PA: US Army War College, March 17, 1999.

Gough, Susan L. *The Evolution of Strategic Influence.* Carlisle Barracks, PA: US Army War College, January 30, 2004.

Joint Chiefs of Staff. *CJSC PLANORD, Influenza Pandemic*, November 14, 2005.

Joint Staff. *CJCSM 3500.04D, Universal Joint Task List (UJTL).* Washington, DC: Government Printing Office, August 1, 2005.

Legal Information Institute. "TITLE 22 > CHAPTER 18 > SUBCHAPTER V > § 1461." In *U.S. Code Collection,* Cornell University Law School, January 3, 2007. http://www.law.cornell.edu/uscode/22/usc_sec_22_00001461----000-.html (Accessed May 8, 2008).

MARFOR Katrina Staff. "USMC Operations in Support of Hurricane Katrina Relief." MARFOR Katrina Lessons Learned Staff Briefing, September, 2005.

McKinney, Cynthia A. *Supplementary Report to the Findings of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina,* February 6, 2006

MOD 1 to CDRUSNORTHCOM EXECUTION ORDER (EXORD) for the Employment of Title 10 Forces within the JTF-KATRINA JOA to Provide Humanitarian Assistance in Support of FEMA. USNORTHCOM, 07 September 2005.

MOD 14 to CDRUSNORTHCOM EXORD for Defense Support to Civil Authorities (DSCA) in Support of FEMA Disaster Relief Operations for Hurricane Katrina. USNORTHCOM, 05 1630Z SEP 05.

OPNAV NOC. Hurricanes Rita and Katrina Update Brief, 24 2200Z SEP 05.

The Role of Information Operations Campaigns in Shaping a Political Reality: The American Experience as an Example. January 11, 2007

Rohm, Fredric W, Jr. "Merging IO and PSYOP." January 11, 2007.

Turabian, Kate L. *A Manual for Writers.* 7th ed. Chicago: University of Chicago Press. 2007.

U.S. Army. Command and General Staff College.. ST 20-10, *Master of Military Art and Science (MMAS) Research and Thesis.* Ft. Leavenworth, KS: USA CGSC, July,2006.

US Army Corps of Engineers (USACE). *USACE Operations Center (UOC) Update Brief*, 23 0900 September 2005.

USCENTCOM J3. *USCENTCOM PI CONPLAN Briefing.* March 13, 2006.

US Department of the Army (?). *CMOC Guide.* Fort Bragg, NC: USACAPOC (?), January 24, 2002.

US Department of Homeland Security. *Hurricane Rita DHS SITREP #6*, 22 0600 September 2005.

US Department of the Navy. "USMC Support to Hurricane Katrina: In-progress Update." Center for Naval Analysis Briefing, December 14, 2005.

USFORSCOM G3. FRAGO 18 to FORSCOM EXORD in Support of Hurricane Katrina, 13 1941Z SEP 05.

USFORSCOM G3. FORSCOM EXORD ISO FEMA/NORTHCOM for Tropical Storm Rita, 20 0522Z SEP 05.

USFORSCOM G3. FORSCOM Requirements/Orders Synchronization Matrix, 11 1808 SEP 05.

USFORSCOM G3. FORSCOM WARNORD for Tropical Storm Rita, 18 2354Z SEP 05

USFORSCOM G3. FORSCOM WARNORD#2 for Tropical Storm Rita, 20 1254Z SEP 05.

USNORTHCOM J3. Mod 13 to Operational /DOD Support for Disaster Relief Operations EXORD, 04 1600Z SEP 05.

USNORTHCOM J3. Operational /DOD Support for Disaster Relief Operations EXORD, 26 1930Z AUG 05.

Washington, Ollie, Jr. *The Legal and Ethical Implications of Information Operations.* Carlisle Barracks, PA: US Army War College, April 10, 2001.

Weatherford, D.J. *9th PSYOP Information Brief.* August, 2007.

Wingfield, Thomas C. and James B. Michael. *An Introduction to Legal Aspects of Operations in Cyberspace.* Monterey, CA: Naval Post Graduate School, April 28, 2004.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

O. Shawn Cupp, Chair
Department of Logistics and Resource Operations (DLRO)
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

LTC Prisco A. Hernandez, Reader
Director, Reserve Component Programs--Army National Guard
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

LTC Robert F. Foley, Second Reader
Chief, Leader Development, Education and Training Division (LDE&T)
U.S. Army Information Operations Proponent (USAIOP)
950 Bluntville Ave, Building 391.
Fort Leavenworth, KS 66027-1352

Distribution: A